SYNGRESS

Federal Cloud Computing

The Definitive Guide for Cloud Service Providers

Matthew Metheny

Federal Cloud Computing

This page is intentionally left blank

Federal Cloud Computing

The Definitive Guide for Cloud Service Providers

Matthew Metheny

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an Imprint of Elsevier

SYNGRESS®

Acquiring Editor: *Chris Katsaropoulos*
Development Editor: *Meagan White*
Project Manager: *Mohanambal Natarajan*
Designer: *Joanne Blank*

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
Metheny, Matthew.
Federal cloud computing : the definitive guide for cloud service providers / Matthew Metheny—First edition.
pages cm
Summary: "In recent years 'cloud computing' has emerged as a model for providing IT infrastructure, resources and services that has the potential to drive significant value to organizations through increased IT efficiency, agility and innovation. However, Federal agencies who were early adopters of cloud computing have learned that there are many challenges and risks that must be addressed in order to realize these benefits"—Provided by publisher.

Includes bibliographical references and index.
ISBN 978-1-59749-737-4 (pbk.)
1. Cloud computing—Security measure. 2. Web services—Government policy. I. Title.
QA76.585.M48 2012
004.67'82—dc23
2012030642

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

Printed in the United States of America
13 14 15 16 17 10 9 8 7 6 5 4 3 2 1

For information on all Syngress publications visit our werbsite at *www.syngress.com*

Excerpts from Federal Information Processing Standards, Special Publications, and Interagency Reports referenced in this book are courtesy of the National Institute of Standards and Technology.

This book is dedicated to my wonderful wife. Her support in giving me the opportunity to write this book cannot be expressed in simple words. For her continuous patience, encouragement, and for those times of sacrifice. For her inspiration and incredible love for reading and editing, even when the subject matter may not have been of interest to her.

To my dear, loving wife Erin.

Thank you for tirelessly standing by my side and supporting me every step of the way. There are many times in one's life where the task may seem too difficult, but having someone like you there as a guiding arm to encourage and to consult has been a blessing.

You have always been there when the times were challenging. It is with great honor to share this accomplishment with you.

To my wife, with love.

This page is intentionally left blank

In memory of Ron Knode.

Ron was a gift that left an impression of a smile, kind words, encouragement, and a unique way to make one think and see in a different perspective. I feel extremely honored to have had the opportunity to know and be mentored by Ron.

Ron, you have left an impression on many that will never be forgotten.

This page is intentionally left blank

Contents

This page is intentionally left blank

About the Author

Matthew Metheny, PMP, CISSP, CAP, CISA, CSSLP, CRISC, CCSK, is the founder of One Enterprise Consulting Group, LLC (1ECG), a privately held consulting firm that specializes in providing professional services that include cloud strategy and architecture, cloud security assessments, cloud migration, and cloud computing training. Mr. Metheny is a member of the Board of Directors for the Cloud Security Alliance (CSA) Washington, DC Metro Chapter, the CloudTrust Protocol (CTP) Working Group Co-Chair, and is a CSA-certified instructor for the Certificate of Cloud Security Knowledge (CCSK). Prior to 1ECG, Mr. Metheny held senior-level program management and executive-level positions with various consulting firms supporting both the federal government and the private sector with a focus on governance, risk management, emerging technologies, and security compliance. In addition, he is the founder of FedRAMP.net, which is focused on supporting cloud service providers and federal agencies with addressing the requirements of the Federal Risk and Authorization Management Program (FedRAMP). Mr. Metheny holds a Master of Science degree in Information Assurance from the University of Maryland University College (UMUC) and multiple internationally recognized certifications.

This page is intentionally left blank

About the Technical Editor

Janis Orsino is an IT security consultant with more than two decades experience delivering technology and business consulting services for the U.S. federal government, in both civilian and defense sectors. She is presently a Senior Managing Consultant with IBM Global Business Services', U.S. Federal Cybersecurity and Privacy Consulting Practice.

From 2009 to 2011, during a contract assignment with the Defense-wide Information Assurance Program, Janis helped to shape the Federal Risk and Authorization Management Program (FedRAMP) from its inception as a key advisor to the DoD Joint Authorization Board. She was also engaged in the cloud computing security guidance development efforts of the Federal CIO Council's Information Security and Identity Management Committee, Network and Infrastructure Security Subcommittee.

Janis holds a Bachelor of Science degree in Social Psychology from Park University, a Graduate Certificate in Legal Studies from The George Washington University, and a string of industry certifications, including Certified Information Systems Security Professional (CISSP), Certified Information Systems Manager (CISM), Certified in Risk and Information Systems Control (CRISC), GIAC Security Leadership Certification (GSLC) and the Certificate of Cloud Security Knowledge (CCSK).

This page is intentionally left blank

Foreword by William Corrington

In recent years "cloud computing" has emerged as a model for providing IT infrastructure, resources and services that has thepotential to drive significant value to organizations through increased IT efficiency, agility and innovation. However, Federal agencies who were early adopters of cloud computing have learned that there are many challenges and risks that must be addressed in order to realize these benefits.

These early adopters have learned that the use of a Cloud Service Provider (CSP) represents a fundamental shift in how IT assets are deployed and delivered on a day-to-day basis. Successful adoption of cloud computing requires a change in approach to (among other things) security, privacy, end-user support, operations, acquisition and contract management.Challenges exist for CSPs as well. Many players in this emerging marketplace are new to doing business with the Federal government. As a result, they not only need to learn the nuances of the Federal acquisition processes, they must also address a myriad of security, privacy and certification requirements that are specific to Federal customers.

In order to mitigate these challenges and to catalyze the adoption of cloud computing within the Federal government, the Federal Cloud Computing Strategy was released on February 8, 2011. The National Institute of Standards and Technology (NIST) and the General Services Administration (GSA) have key roles in the implementation of this "Cloud First" strategy. NIST has developed a number of Special Publications that provide definitions, architectural standards and roadmaps for cloud computing. GSA has developed the Federal Risk and Authorization Management Program (FedRAMP) to define security, auditing, continuous monitoring and other operational requirements for Federal agency use of cloud computing.

I admire the groundbreaking initiatives that have been spearheaded by NIST and GSA. And yet, these efforts have created a new landscape with its own set of twists and turns that must be navigated by both Federal agencies and CSPs wishing to serve the Federal marketplace. What has been missing so far is a definitive reference guide that will allow anyone with a stake in Federal IT to quickly ascend the learning curve associated with the goals, objectives, implementation and operational aspects of the Federal Cloud Computing Strategy. Mr. Metheny's book fills this gap by providing a comprehensive view of how and where cloud computing fits in the Federal government and how the critical components of the Cloud First strategy will work together in a complementary fashion.

I believe that this book will prove to be an invaluable resource to anyone who needs to successfully navigate the brave new world of Federal cloud computing. Cloud Service Providers (CSPs) will gain an understanding of the security and operational requirements that must be met in order to provide cloud-based services to Federal agencies. Cloud auditors who wish to provide services to Federal agencies or CSPs will learn the detailed requirements for becoming a Third Party Assessment Organization (3PAO). Federal agency CIOs, CTOs and CISOs will benefit from greater clarity regarding the impacts that the move to cloud computing will have on their existing IT strategy and operations.

The Cloud First strategy is a critical component of broader efforts that are underway to transform Federal IT in the 21st century. This book will provide excellent guidance to everyone who wishes to undertake that journey.

William Corrington
Founder and Chief Cloud Strategist
Stony Point Enterprises
(Former Chief Technology Officer
at the US Department of Interior)

Foreword by Jim Reavis

Cloud computing is an epochal change in the use of technology by mankind. Broadly considered, it represents the transition towards the use of compute as a utility, with profound implications. Just as when nations became electrified, the dawn of new industries, reorganization of societies and other unexpected outcomes are surely at our doorstep. Access to supercomputer capabilities, previously only available to small groups of people with millions of dollars, is now available to all.

The ability for individuals, small businesses and large enterprises to have "on demand" access to a virtually unlimited supply of compute power and storage challenges our ability to innovate. From discovering new drugs to unlocking the mysteries of the universe to finding better solutions for the human condition, we are only limited by our imagination.

Governments are no different than any other organization in their propensity to be impacted by, and leverage the cloud. The very largest problems facing governments have the potential to be solved in large part by the cloud. Cloud will also force government agencies to be more transparent and collaborative with the information that forms the backbone of their services. At the same time, a rush to adopt cloud computing without a sound understanding of its potential and risks could prove a devastating setback. This book, "Federal Cloud Computing: The Definitive Guide for Cloud Service Providers" is a timely addition to our shared knowledge of what cloud computing is, the inherent risks, regulatory requirements and the ecosystem of standards and best practices.

Cloud Security Alliance is a not-for-profit organization that is the leading global force in building trust within cloud computing. We congratulate author and CSA member Matthew Metheny for his excellent contribution to the topic of cloud computing within the US Federal government. We feel this book is must reading for anyone interested in information technology within our government. Both government consumers and providers must understand the regulatory requirements, the processes for making cloud services available and best practices to mitigate risks and operate cloud systems securely.

Cloud computing is not only in our future, but is here today. Whatever role you play in this topic, you have a mandate to find strategies to securely adopt cloud in an agile manner. "Federal Cloud Computing: The Definitive Guide for Cloud Service Providers" is an excellent coach to help define those strategies.

Best,

Jim Reavis
Executive Director, Cloud Security Alliance

This page is intentionally left blank

CHAPTER

1 Introduction to the Federal Cloud Computing Strategy

INFORMATION IN THIS CHAPTER:

- Introduction
- A Historical View of Federal IT
- Cloud Computing: Drivers in Federal IT Transformation
- Decision Framework for Cloud Migration

INTRODUCTION

In February of 2011, the former US Chief Information Officer (CIO), Vivek Kundra, published the *Federal Cloud Computing Strategy*, herein referred to as the "*Cloud Strategy*."[1] The *Cloud Strategy*, as illustrated in Figure 1.1, was one of six major components of the US CIO's roadmap to the cloud as defined in the *25 Point Implementation Plan to Reform Federal Information Technology Management*.

In the *Cloud Strategy*, the federal government's strategic approach for the adoption of cloud computing technologies was described, including the potential benefits, considerations, and trade-offs [1]. The strategy also provided a decision framework for federal agencies to use in outlining their plan for using cloud computing to improve their efficient use of information technology (IT) investments to support their missions by leveraging shared infrastructures and economies of scale. This framework focused on changing how the government approaches IT and how it could effectively integrate cloud services into its existing IT portfolio.

The *Cloud Strategy* established a set of basic principles and guidelines through which decision-makers within federal agencies could use it to accelerate their secure adoption of cloud services. Through the strategy, federal agencies were empowered with the responsibility for making their own decision on "*what*" and "*how*" to migrate to the cloud in support of the government-wide Cloud First policy. The Cloud First policy was established to create the momentum for federal agencies to proactively adopt

[1] *Federal Cloud Computing Strategy*. Available from: http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf.

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00001-0

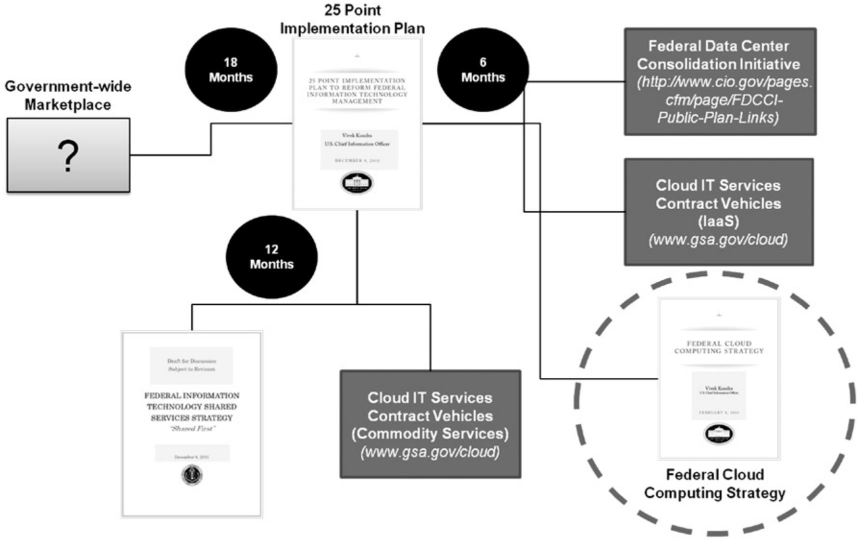

25 Point
Implementation Plan
25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL INFORMATION TECHNOLOGY MANAGEMENT
Vivek Kundra
U.S. Chief Information Officer
18 Months
6 Months
12 Months
Government-wide Marketplace
?
Federal Data Center Consolidation Initiative (http://www.cio.gov/pages.cfm/page/FDCCI-Public-Plan-Links)
Cloud IT Services Contract Vehicles (IaaS) (www.gsa.gov/cloud)
Draft for Discussion
Subject to Revision
FEDERAL INFORMATION TECHNOLOGY SHARED SERVICES STRATEGY
"Shared First"
Cloud IT Services Contract Vehicles (Commodity Services) (www.gsa.gov/cloud)
FEDERAL CLOUD COMPUTING STRATEGY
Vivek Kundra
Federal Cloud Computing Strategy

FIGURE 1.1 25 Point Implementation IT Reform Plan—"Roadmap to the Cloud"

cloud computing services by requiring them to begin with the selection of three "*cloud-ready*"[2] IT services that could be migrated to secure and reliable cloud solutions.

In the section *Decision Framework for Cloud Migration*, a three-step framework described the foundational elements that were identified as being necessary for building a successful migration plan.[3] In addition, the Cloud First policy gave federal agencies the opportunity to exercise their migration plans[4] and develop and share "*lessons learned*" from their experiences. The policy also established the requirement for a program[5] to be developed that would encourage Cloud Service Providers

[2] Cloud readiness was one dimension for making risk-based decisions when determining which IT service to migrate to the cloud. Readiness included factors such as: security, service characteristics, market characteristics, network infrastructure, application, and data readiness, government readiness, and technology lifecycle.

[3] From Kundra, V. *Federal Cloud Computing Strategy*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. *Each migration plan includes: major milestones, execution risks, adoption targets, resource requirements, and retirement plans for legacy services after the cloud service is online.*

[4] From Kundra, V. *25 Point Implementation Plan to Reform Federal Information Technology Management*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010. "*The three-party strategy on cloud computing technology will evolve around using commercial cloud technologies where feasible, launching government clouds, and utilizing regional clouds with state and local government where appropriate.*"

[5] The Federal Risk and Authorization Management Program (FedRAMP) will be is discussed in detail in Chapter 8, FedRAMP Primer, and Chapter 9, The FedRAMP Cloud Computing Security Requirements.

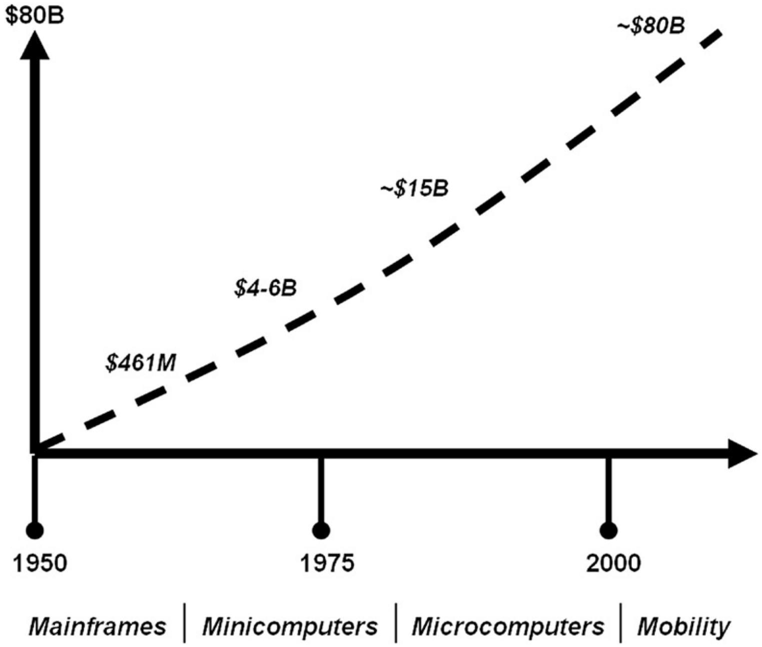


FIGURE 1.2 History of Federal IT Portfolio

(CSPs) to meet federal security and privacy requirements through the development of "*government-ready*" cloud services.[6]

The federal government's shift, from a traditional asset-based model focused on acquiring IT, to a service-based model offered by cloud computing is not only a change in the technology, but also a cultural change in the organization itself. The "shift" towards cloud services also requires organizational changes for managing the people and processes that are needed for procuring and provisioning cloud services. Cloud computing places an increased importance on how technology is planned, selected, and integrated.[7] The new service-based approach to IT requires federal agencies to learn how to manage services rather than assets. To effectively provision cloud services so that there can be an achieved optimization of resources, federal agencies will have to link the benefits of cloud computing to their strategic plans.[8]

[6] "Government-ready" cloud services refer to those that can satisfy a broad range of federal security and privacy requirements to include: statutory compliance, data security, protection of privacy-related information, integrity, access controls, and governance and security management.

[7] Office of Management and Budget (OMB) Circular A-11, Part 7—"*Planning, Budgeting, Acquisition, and Management of Capital Assets.*" Available from: http://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc.

[8] Office of Management and Budget (OMB) Circular A-11, Part 6—"*Preparation and Submission of Strategic Plans, Annual Performance Plans, and Annual Program Performance Reports.*" Available from: http://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc.

In addition, federal agencies will also have to establish new governance processes and practices to ensure the adoption of secure cloud services adheres to the federal information security and privacy requirements.

NOTE

Importance of Federal IT Strategic Planning in the Adoption of Cloud Computing

Government-wide IT strategic planning for information and information technology management has been highlighted as a systematic challenge almost since federal agencies began using IT. As early as 1960,[9] the US General Accounting Office (GAO)[10] " … call(ed) attention to the need for more positive central planning of a long-range nature within the executive branch of the government to promote the maximum degree of efficiency, economy, and effectiveness in the administration and management of costly automatic data processing facilities" [2].

However, it was not until 1980[11] that the management of federal IT authority was centralized within the federal government. The Office of Management and Budget (OMB) was given government-wide responsibility to "oversee the use of information resources to improve the efficiency and effectiveness of governmental operations to serve agency missions" [3]. Federal agencies were also required to designate a senior agency official (also known as the Agency Chief Information Officer (CIO)) to be responsible for information resource management (IRM)[12] at the department and agency level. As the government-wide IRM activities evolved, Agency CIOs were also given additional responsibilities in developing "strategic plans[13] for all [departmental and agency] information and information technology management functions" [4].

IT Strategic Plans[14] play an important role in the adoption of cloud computing specifically when planning the expected improvements in productivity, efficiency, and

[9] *Review of Automatic Data Processing Developments in the Federal Government.*

[10] The GAO was established under the Budget and Accounting Act of 1921. In July 7, 2007, the General Accounting Office was changed to the Government Accountability Office.

[11] *Paperwork Reduction Act of 1980.* Available from: http://www.archives.gov/federal-register/laws/paperwork-reduction/.

[12] From Melvin, V. "*Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*". Washington: US Government Accountability Office; 2011. "*IRM is the process of managing information resources to accomplish agency missions and to improve agency performance.*"

[13] From Office of Management and Budget (OMB). Revision of OMB Circular No. A-130, Transmittal No. 4 [Internet]. Washington, DC: Executive Office of the President, Office of Management and Budget [cited 2012 August 27]. Available from: http://www.whitehouse.gov/omb/fedreg_a130notice. "*The IRM Strategic Plan is the agency's IT vision or roadmap that will align its information resources with its business strategies and investment decisions.*"

[14] From Office of Management and Budget (OMB). Revision of OMB Circular No. A-130, Transmittal No. 4 [Internet]. Washington, DC: Executive Office of the President, Office of Management and Budget [cited 2012 August 27]. Available from: http://www.whitehouse.gov/omb/fedreg_a130notice. "*The Clinger-Cohen Act directs agencies to work together towards the common goal of using information technology to improve the productivity, effectiveness, and efficiency of Federal programs and to promote an interoperable, secure, and shared government-wide information resources infrastructure.*"

effectiveness. Agency CIOs will need to be more effective in aligning IT Strategic Plans with Agency Strategic Plans[15] that enable the development and monitoring of performance metrics used to evaluate the business value of cloud services. Therefore, the IT strategic planning process used by Agency CIOs will need to emphasize the establishment of criteria that are more focused on objectively and quantitatively measuring the benefits of the investment of cloud computing technologies across the department and agency.

A HISTORICAL VIEW OF FEDERAL IT

In the Cloud Strategy, the federal IT environment was characterized as having "low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times" [1]. This characterization was the result of an accumulation of issues stemming from years of mismanagement and the over-capitalization of IT.

In this section, we will focus on introducing several key historical points within the federal government where the adoption of IT produced trends that led to the growth in the federal IT budget. Figure 1.2 provides a high-level illustration that depicts how the federal government's IT budget and portfolio changed with the transition to newer technologies.

Our review will begin with mainframe computing (*a highly centralized environment*) and end with the federal government's transition to mobility (*a highly decentralized environment*). For completeness, the review will also include a brief discussion of the evolution of federal IT laws and policies developed over time to manage issues across the federal government such as acquisition, governance, privacy, and security.

The Early Years and the Mainframe Era

The origins of modern computing[16] can be directly linked to the US government. As the first significant[17] user of computers, the US government consequently became

[15] From Office of Management and Budget (OMB). Revision of OMB Circular No. A-130, Transmittal No. 4 [Internet]. Washington, DC: Executive Office of the President, Office of Management and Budget [cited 2012 August 27]. Available from: http://www.whitehouse.gov/omb/fedreg_a130notice. *"IRM Strategic Plans should support the Agency Strategic Plans, describing how information resources will help accomplish agency missions and ensuring that IRM decisions are integrated with organizational planning, budget, financial management, procurement, human resources management, and program decisions."*

[16] University of Pennsylvania. John W. Mauchly and the Development of the ENIAC Computer. 2003 April 23. Available from: http://www.library.upenn.edu/exhibits/rbm/mauchly/jwmintro.html.

[17] Project Whirlwind Reports. Available from: http://dome.mit.edu/handle/1721.3/37456.

one of the primary sources for most of the funding for the innovation and research in computing technology. In the early years, computers were very expensive, slow, inefficient, and took up a sizeable footprint,[18] making them impractical for use outside of the U.S. government or research facilities. Despite limitations, the U.S. government continued to finance the development and advancement of computer technologies. Originally, computers were only used for military applications.[19] However, this initial investment would serve to establish the beginnings of an industry that would shape how the federal government would use and operate computers today.

The first digital computers[20] used by the federal government before the 1950s were primarily used for scientific and defense purposes.[21] Although from the late 1940s to early 1950s the federal government's interest began to change their focus on using computers to address broader business challenges. In 1951, the emergence of the UNIVersal Automatic Computer (UNIVAC) I[22] created opportunities to use computers for application outside of the US Department of Defense (DoD), and the UNIVAC became the first business computer purchased by the Bureau of the Census[23] to be used for the population and economic censuses. During the remainder of the 1950s, several other civilian federal agencies also began to acquire[24] and use mainframes to supplement and support mission-specific operations. Federal agencies saw these computers as a useful tool for improving the productivity of more resource-intensive business support functions. For example, mainframes were used to more efficiently and accurately calculate tax returns (Internal Revenue Service), to calculate social security benefits (Social Security Administration), and to generate labor statistics (US Department of Labor).

The federal government's acquisition activity for computers began to increase significantly as the shift changed from using mainframes for basic business

[18] From Margherio, L., Henry, D., Cooke, S., and Montes, S. *The Emerging Digital Economy*. Washington: US Department of Commerce, Economics and Statistics Administration; 1998. *In 1946, the world's first programmable computer, the Electronic Numerical Integrator and Computer (ENIAC), stood 10 ft tall, stretched 150 ft wide, cost millions of dollars, and could only execute up to 5000 operations per second.*

[19] US Army Research Laboratory (ARL) Computing History. Available from http://www.arl.army.mil/www/default.cfm?page=148.

[20] US Census Bureau. History: Univac I. Census History Staff. 2011 June 30. Available from: http://www.census.gov/history/www/innovations/technology/univac_i.html.

[21] *Problems Found With Government Acquisition And Use of Computer From November 1965 to December 1976*. Available from: http://www.gao.gov/assets/120/116645.pdf.

[22] Fay, F.X. The engineers get together … Look back at the future. The Norwalk Hour. 1996 October 25. Available from: http://www.rowaytonhistoricalsociety.org/firstcomputer.html.

[23] US Census Bureau. History: Univac I. Census History Staff. 2011 Jun 30. Available from: http://www.census.gov/history/www/innovations/technology/univac_i.html.

[24] From Comptroller General of the United States. Problems Found With Government Acquisition And Use of Computer From November 1965 to December 1976. Washington: US General Accounting Office; 1977. *Between 1955 and 1960, the number of computers in the federal government increased from 45 to 531.*

support functions to more complex mission-specific applications.[25] As a result, the federal government increased its purchasing of computers from 531 computers (or $464 million) in 1960 to over 5277 computers (or an estimated $4 to $6 billion[26] in capital expenditures) in 1970 [5]. The significant increase in the computer inventory was primarily the result of federal agencies having the purchasing power to procure resources needed to support their own individual needs and requirements.

As the federal government's mainframe inventory grew, federal agencies began to face challenges associated with vendor and technology lock-in.[27] As was customary in industry pricing practices at that time, software and engineering support services were bundled with the hardware [5]. This bundling resulted in federal agencies being locked into their mainframe vendors, making the migration between technologies a challenge because the manufacturer had full control over the entire stack, from the proprietary mainframe hardware platform to the software applications. In the 1980s, after the pricing practices began to change as major mainframe manufacturers started to unbundle the hardware, software, and engineering support services, the federal government was faced with a limited number of companies in the mainframe market.[28] This made it even more difficult for federal agencies to modernize their legacy applications.[29]

Shifting to Minicomputer

The advancement in hardware technology introduced the integrated circuit and the market evolved to midsized computers. Throughout the 1970s and 1980s, the federal government also began to shift away from using mainframes and began acquiring minicomputers. For the federal government, minicomputers provided a more efficient improvement in central processing and "time sharing" capabilities offering a much lower cost and size, thereby enabling them to be more broadly available across the federal government. By 1974, as illustrated in Figure 1.3, more than fifty (50)

[25] From Comptroller General of the United States. Problems Found With Government Acquisition and Use of Computers From November 1965 to December 1976. Washington: US General Accounting Office; 1977. *Example applications included: automating clinical laboratory processing (US Department of Veteran Affairs); managing housing grants (US Department of Housing and Urban Development); storing and retrieving criminal data (US Department of Justice); and predicting crop level (US Department of Agriculture).*

[26] $2 billion was being spent annually on software.

[27] Brown, K., Adler, S.M., Irvine, R.L., Resnikoff, D.A., Simmons, I., Tierney, J.J. *United States memorandum on the 1969 case*. Washington: US Department of Justice; 1995. Available from: http://www.justice.gov/atr/cases/f0800/0810.htm.

[28] The top vendor of IBM-compatible procurements was IBM with 65% of the total obligated federal dollars.

[29] From US General Accounting Office (GAO). Mainframe procurements: Statistics showing how and what the government is acquiring. Washington: US General Accounting Office; 1990. "*35 federal agencies had 3,255 procurements and obligated $1,943.1 million for mainframe computers and mainframe peripherals during the 3 ½ fiscal years ending in March 1989.*"

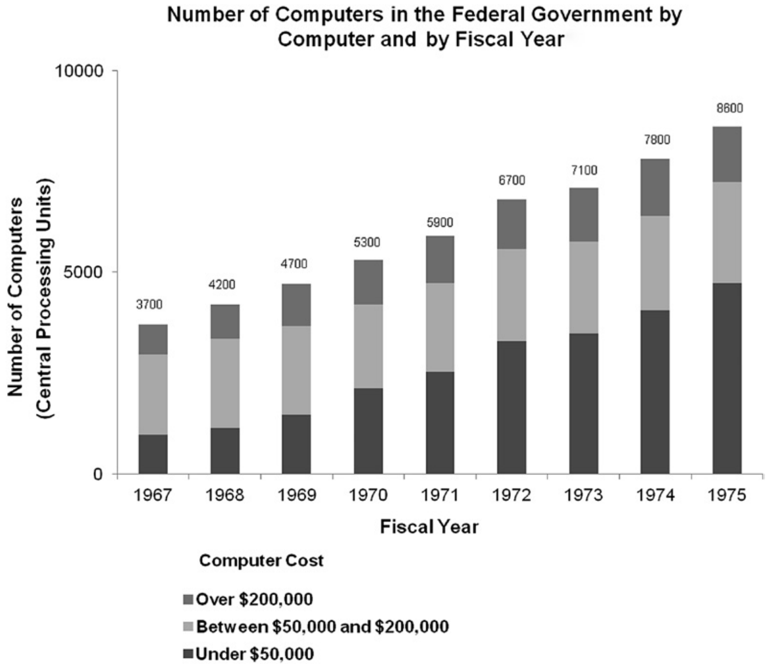


FIGURE 1.3 Comparison of Computers Purchased Between 1967 and 1975 [6]

percent of the computers in the federal government cost less than $50,000 and the inventory exceeded 8600.

Minicomputers offered the federal government greater opportunities to use technology to increase productivity through the use of automation to lower economic costs in areas where repetitive activities were being performed manually. As an example, minicomputers were used by the National Weather Service to automate forecast offices [6], the Internal Revenue Service for electronically preparing individual tax returns [7], the Federal Aviation Administration to automate air traffic control functions, and the US Department of Justice to automate legal information and retrieval [8].

Decentralization: The Microcomputer (“Personal Computer”)

By the mid-1970s, the emergence of the microcomputer decentralized computing and empowered end-users within the federal government. The significantly lower cost gave federal agencies the ability to extend microcomputers to a broader workforce with hopes of improving productivity across the federal government. For example, in 1983, the US General Services Administration (GSA) began opening Office of Technology Plus (OTP) stores (“GSA microcomputer stores”) to make it easier for federal agencies to procure microcomputers by streamlining the buying process.

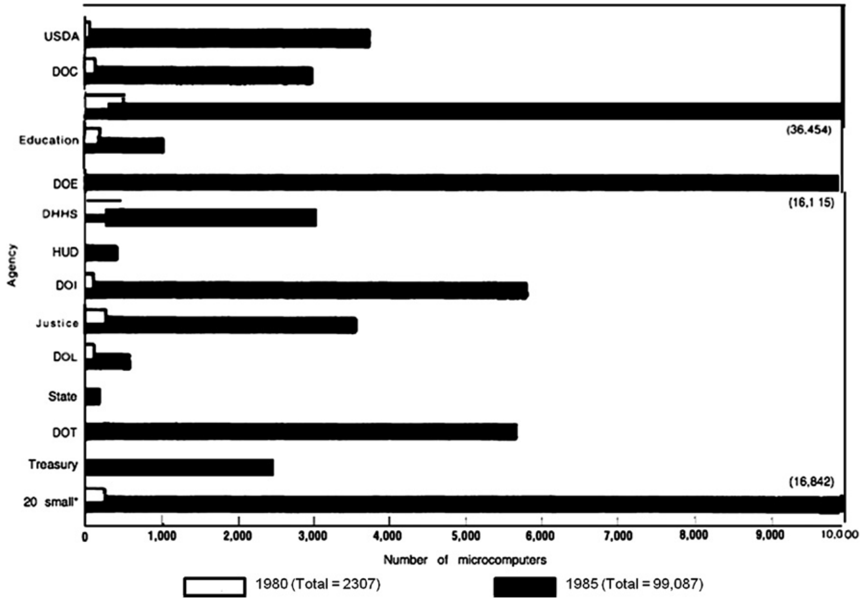


FIGURE 1.4 Comparison of Microcomputers Purchased Between 1980–1985 [2]

Microcomputer adoption continued to gain significant momentum in the mid-1980s. By 1986, the federal government had amassed the largest inventory of computer equipment in the world, with a cumulative IT budget of over $60 billion between fiscal years 1982–1986.[30] As illustrated in Figure 1.4, the government-wide microcomputer inventory increased from 2307 in 1980 to 99,087 in 1985.

The accelerated growth in the IT inventory was also challenged with an underdeveloped information resource management (IRM) practice[31] that began to impact the overall value and performance of the federal government's return on its IT investment. The federal government saw impacts in areas such as the efficiency in delivering citizen services; maintaining the security and privacy of information stored in computerized form; and the quality of government IT management [2].

[30] The federal government 2011 IT budget was approximately $80 billion a year.

[31] From US Congress, Office of Technology Assessment (OTA). Federal Government information technology: Management, security, and congressional oversight. Washington: US Government Printing Office; 1986. *IRM brings together under one management structure previously disparate functions and reorients the focus of information systems management from hardware and procedures to the information itself.*

Transitioning to Mobility

Fast forwarding to today, the federal government operates in a more complex world that includes a mix of technologies. The emergence of different types of platforms (e.g., smartphones and tablet computers) offers the federal government new opportunities to improve its efficiency, while at the same time it faces the challenge of ensuring the security and privacy of vast amounts of digital information. With a broad array of mobile devices available, the federal government is starting to embrace the investment[32] in mobility. The expansive adoption of technologies that enable mobility will require the federal government to confront potential new challenges relating to the management of these different devices, the supporting infrastructures, and the software applications. In addition, federal agencies will need to learn to manage the continued growth in mobile applications[33] and services[34] to optimize the efficient use of these technologies and make their "business case" for mobility.

Many federal agencies have already become accustomed to using mobile computing devices (e.g., laptops) through their experience in teleworking.[35] Federal agencies are also continuing to explore opportunities that would maximize the benefits gained through the use of other mobile devices to enable them to operate more cost-effectively and efficiently. Therefore, as federal agencies make the transition to be more mobile[36] and increase their usage of mobile computing devices, they will be required to be more proficient at both managing and securing different types of devices. This also means federal agencies will need to learn how to *select*, *provision*, and *manage* secure cloud services that will be leveraged as more information is moved into digital services so they can be accessed by endpoint devices anytime, anywhere.

[32] The National Security Agency (NSA) released a version of the Android operating system through the Security Enhanced (SE) Android project. Available from: http://selinuxproject.org/page/SEAndroid.

[33] Mobile Gov Wiki was designed as a collaborative platform for building a mobile strategy. Available from: http://mobilegovwiki.howto.gov/.

[34] From Federal Chief Information Officers Council. Federal Mobility Strategy [Internet]. Washington, DC: Office of Management and Budget [cited 2011 April 30]. Available from: http://www.cio.gov/pages.cfm/page/Federal-Mobility-Strategy. *In January 11, 2012, the Federal CIO launched the Federal Mobility Strategy development to focus on accelerating the Federal government's adoption of mobile technologies and services.*

[35] In December 9, 2010, the Telework Enhancement Act of 2010 (P.L. 111-192) was signed into law requiring federal agencies to include as part of their telework programs an assurance of adequate information and security protection. OMB 11-27,"*Implementing the Telework Enhancement Act of 2010: Security Guidelines*" established the guidelines on security requirements.

[36] From Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. "*The Digital Government Strategy incorporates a broad range of input from government practitioners, the public, and private-sector experts. Two cross-governmental working groups—the Mobility Strategy and Web Reform Task Forces—provided guidance and recommendations for building a digital government.*"

Evolution of Federal IT Policy

In the previous section we briefly explored the history of IT adoption within the federal government from *mainframes* to *mobility*. In this section, the focus will include highlights of key federal IT laws and policies. Many of the laws and IT policies were developed to govern the general practices for using IT within the federal government; others addressed more specific topics such as security and privacy. Tables 1.1 and 1.2 provide a detailed timeline of how the current IT policy framework evolved over time to address government-wide oversight and the management of IT-related issues and challenges. However, the policy framework established by Congress and the executive branch to control, oversee, and encourage the effective management and efficient use of IT was overtaken by the rapid pace at which new technology applications, issues, and opportunities were being generated or were not envisioned at the time of enactment or development of the policies [2].

The early adoption of IT was a significantly small portion of the annual budget in the 1960s. Therefore, purchasing power was performed in an isolated, decentralized manner, where each federal agency was given the flexibility to make its own buying decisions, including determining the types of technologies that were needed to meet its requirements. It was not until the mid-1960s that Congress took actions to improve the efficiency and effective use of IT across the federal government.

The enactment of the Brooks Act of 1965[37] was the first significant legislation focusing specifically on federal IT issues by establishing an oversight and management structure. The Brooks Act[38] outlined the major roles and responsibilities for the government-wide management of IT, which mostly operate under the same functions today (with an exception (*) noted):

- the US General Services Administration (GSA)* was given the authority and responsibility over the purchase, lease, maintenance, operation, and utilization of automated data processing (ADP) equipment;
- OMB was given the fiscal and policy control; and
- the Secretary of Commerce, through the National Bureau of Standards (NBS), now known as the National Institute of Standards and Technology (NIST), was directed with setting technical standards and guidelines.

The Brooks Act was established to reform federal IT by addressing three main issues: (1) competitiveness and "best value" through centralized government purchasing, (2) acquisition and IT management, and (3) common computing standards that would enable federal agencies to share information. In 1996, the enactment of the Information Technology Management Reform Act (ITMRA) of 1996 (now known as the Clinger-Cohen Act) repealed the Brooks Act, effectively eliminating GSA's role as the primary federal agency for setting policy and regulations for federal IT procurements. Instead, the Clinger-Cohen Act delegated this authority to the newly created role of the

[37] Brooks Act. Available from: www.itl.nist.gov/History%20Documents/Brooks%20Act.pdf.
[38] 89th Congress. Public Law 89-306, Brooks Act of 1965. Washington: US Congress; 1965.

Table 1.1 Timeline of Major Federal IT Legislation

1949 – *Federal Property and Administrative Services Act of 1949* – Established the US General Services Administration (GSA).

1950 – *Federal Records Act of 1950 (P.L. 81-754)* – Established the framework for records management programs in federal agencies.

1965 – *Brooks Act of 1965 (P.L. 89-306)* – Designated GSA with the authority and responsibility for ADP equipment, OMB with fiscal and policy control, and NIST the responsibility for standards and guidelines development.

1974 – *Privacy Act of 1974 (P.L. 93-579)* – Governed the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

1980 – *Paperwork Reduction Act of 1980 (P.L. 96-511)* – Established the OMB, Office of Information Regulator Affairs (OIRA) and gave authority to regulate federal information collection from the public and to establish information policies.

1984 – *Competition in Contracting Act of 1984 (P.L. 98-369)* – Established policy to encourage competition resulting in savings to the federal government through competitive pricing.

1987 – *Computer Security Act of 1987 (P.L. 100-235)* – Established minimum acceptable security practices for federal computer systems and reaffirmed the responsibility of NIST for standards and guidelines development.

1988 – *Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503)* – Established new provisions regulating use of Privacy Act records in performing certain types of computer matching.

1993 – *Government Performance and Results Act of 1993 (P.L. 103-62)* – Required federal agencies to develop multi-year strategic plans, annual performance plans, and evaluate and report on the results annually.

1994 – *Federal Acquisition Streamlining Act of 1994 (P.L. 103-355)* – Established the US General Services Administration (GSA).

1998 – *Government Paperwork Elimination Act of 1998 (P.L. 105-277)* – Established new provisions regulating use of Privacy Act records in performing certain types of computer matching.

2000 – *Government Information Security Reform Act of 2000 (P.L. 106-398)* – Required federal agencies having control over unclassified and national security programs establish an information security management program.

2002 – *E-Government Act of 2002 (P.L. 107-347)* – Enhanced the management and promotion of electronic government services and processes by establishing the Federal Chief Information Officer within OMB. Additionally, the Federal Information Security Management Act (FISMA) was enacted as part of the E-Government Act.

2010 – *GPRA Modernization Act of 2010 (P.L. 111-352)* – Created a more defined performance framework by prescribing a governance structure and improved the connection between plans, programs, and performance information by requiring federal agencies to set clear performance goals that they can accurately measure and publicly report in a more transparent way.

Table 1.2 Timeline of Major Federal IT Policy

1961 – *Policies on Selection and Acquisition of Automatic Data Processing Equipment (OMB Circular A-54):* Outlined policies on selecting ADP equipment to replace and upgrade equipment and acquiring on hand and provides that agencies revalidate the workload and data processing requirements to determine if a reduction can be effected, and determine the possibility of improving the performance of existing facilities through program modifications, rescheduling, or the selective replacement of software or peripheral devices which offer greater efficiency or lower cost.

1979 – *Security of Federal Automated Information Systems (OMB Circular A-71):* Required federal executive departments and agencies to establish automated security programs and develop security plans that would be reviewed by OMB.

1996 – *Implementation of the Information Technology Management Reform Act (OMB Memorandum 96-20:* Designated the chief information officer (CIO) and the role of the General Services Board of Contract Appeals (GSBCA) in information technology protests.

1996 – *Funding Information System Investments (OMB Memorandum 97-02):* Directed the OMB to establish clear and concise direction regarding investments in major information systems, and to enforce that direction through the budget process.

1997 – *Local Telecommunication Services Policy (OMB Memorandum 97-15):* Provided federal agencies the flexibility and responsibility to acquire, operate, manage, and maintain telecommunications resources while taking advantage of the economies of scale and management efficiencies that aggregation of service and acquisitions can produce.

1997 – *Information Technology Architecture (OMB Memorandum 97-16): Provided guidance for federal agencies in the development and implementation of Information Technology Architectures.*

1999 – *Instructions for complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" (OMB Memorandum 99-05): Provided instructions to federal agency to comply with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"*

1999 – *Privacy Policies for Federal Web Sites (OMB Memorandum 99-18): Directed federal agencies to provide guidance and post clear privacy policies on their websites.*

1999 – *Security of Federal Automated Information Resources (OMB Memorandum 99-20): Reminded federal agencies they must assess the risk to their computer system and maintain adequate security commensurate with that risk.*

2000 – *Management of Federal Information Resources (OMB Circular A-130):* Established policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.

2000 – *Incorporating and Funding Security in Information Systems (OMB Memorandum 00-07): Reminded federal agencies of the principles for incorporating and funding security as part of information technology systems and architectures and decision criteria for evaluating security for information systems investments.*

2000 – *Implementation of the Government Paperwork Elimination Act (OMB Memorandum 00-10):* Provided procedures and guidance to implement the Government Paperwork Elimination Act.

2000 – *Privacy Policies and Data Collection on Federal Web Sites (OMB Memorandum 00-13): Reminded federal agencies of their requirement by law and policy to establish clear privacy policies for web activities.*

Table 1.2 Timeline of Major Federal IT Policy (*continued*)

2001 – *Guidance On Implementing the Government Information Security Reform Act (OMB Memorandum 01-08):* Provided guidance on the implement of the Government Information Security Reform Act primarily addresses the program management and evaluation aspects of security. It covers unclassified and national security systems and creates the same management framework for each. At the policy level, the two types of systems remain separate.

2001 – *Guidance for Preparing and Submitting Security Plans of Action and Milestones (OMB Memorandum 02-01): Provided guidance on a standard format for information federal agencies should include in their plan of action and milestones (POA&Ms).*

2003 – *Implementation Guidance for the E-Government Act of 2002 (OMB Memorandum 03-18):* Explained how the E-Government Act fits within existing IT policy, such as OMB Circulars A-11 (Preparation, Submission, and Execution of the Budget) and A-130 (Management of Federal Information Resources).

2003 – *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (OMB Memorandum 03-19):* Provided direction to agencies on implementing FISMA.

2003 – *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (OMB Memorandum 03-22):* Provided information to agencies on implementing the privacy provisions of the E-Government Act of 2002.

2003 – *E-Authentication Guidance for Federal Agencies (OMB Memorandum 04-04):* Required agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication.

2004 – *Maximizing Use of SmartBuy and Avoiding Duplication of Agency Activities with the President's 24 E-Gov Initiatives (OMB Memorandum 04-08):* Enhanced the ability of agencies to manage software and to maximize the federal government's buying power.

2004 – *Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources (OMB Memorandum 04-15):* Provided the required format for agencies to use when submitting internal critical infrastructure protection (CIP) plans.

2004 – *Software Acquisition (OMB Memorandum 04-16): Reminded agencies of policies and procedures covering acquisition of software to support agency operations.*

2004 – *FY 2004 Reporting Instructions for the Federal Information Security Management Act (OMB Memorandum 04-25): Provided direction to agencies for meeting FY 2004 FISMA reporting requirements.*

2004 – *Personal Use Policies and "File Sharing" Technology (OMB Memorandum 04-26): Provided specific actions federal agencies must take to ensure appropriate use of certain technologies used for file sharing across networks.*

2004 – *Policies for Federal Agency Public Websites (OMB Memorandum 05-04): Provided direction for federal agencies in fulfilling the requirements of section 207(f) of the E-Government Act of 2002.*

2005 – *Designation of Senior Agency Officials for Privacy (OMB Memorandum 05-08):* Required agencies to designate a senior official who has the overall agency-wide responsibility for information privacy issues.

2005 – *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (OMB Memorandum 05-15): Provided direction to agencies for meeting FY 2005 FISMA reporting requirements.*

Table 1.2 Timeline of Major Federal IT Policy (*continued*)

2005 – *Improving Information Technology (IT) Project Planning and Execution (OMB Memorandum 05-23): Provided guidance to assist federal agencies in monitoring and improving project planning and execution and fully implementing Earned Value Management Systems (EVMS) for IT projects.*

2005 – *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (OMB Memorandum 05-24):* Provided instructions for the implementation of HSPD-12 and FIPS 201.

2006 – *Safeguarding Personally Identifiable Information (OMB Memorandum 06-15):* Reemphasized federal agency responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and train your employees on their responsibilities in this area.

2006 – *Protection of Sensitive Agency Information (OMB Memorandum 06-16): Provided recommendations for agencies to properly safeguard information assets while using information technology.*

2006 – *Acquisition of Products and Services for Implementing HSPD-12 (OMB Memorandum 06-18): Provided direction for the acquisition of products and services for the implementation of HSPD-12.*

2006 – *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (OMB Memorandum 06-19):* Provided updated guidance on the reporting of security incidents involving personally identifiable information.

2006 – *FY 2006 E-Government Act Reporting Instructions (OMB Memorandum 06-25): Provided for federal agencies annual E-Government reports required under the E-Government Act of 2002.*

2006 – *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (OMB Memorandum 06-20): Provided direction to agencies for meeting FY 2006 FISMA reporting requirements.*

2007 – *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (OMB Memorandum 07-16):* Required agencies to develop and implement a breach notification policy.

2007 – *Ensuring New Acquisitions Include Common Security Configurations (OMB Memorandum 07-18): Provided recommended language for federal agencies to use in solicitations to ensure new acquisitions include common security configuration and information technology providers certify their products operate effectively using these configurations.*

2007 – *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (OMB Memorandum 07-19): Provided direction to agencies for meeting FY 2007 FISMA reporting requirements.*

2008 – *Implementation of Trusted Internet Connections (TIC) (OMB Memorandum 08-05):* Initiated the Trusted Internet Connections (TIC) initiative to optimize individual federal agency network services into a common solution for the federal government.

2008 – *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (OMB Memorandum 08-21): Provided direction to agencies for meeting FY 2008 FISMA reporting requirements.*

2008 – *Guidance on the Federal Desktop Core Configuration (FDCC) (OMB Memorandum 08-22): Required industry and the federal government to use SCAP validated tools with FDCC scanner capabilities to certify product operate correctly with the FDCC configurations.*

Table 1.2 Timeline of Major Federal IT Policy (*continued*)

2008 – *Guidance for Trusted Internet Connection (TIC) Compliance (OMB Memorandum 08-27):* Provided guidance and clarification on coordination with the Department of Homeland Security's (DHS's) National Cyber Security Division (NCSD).

2008 – *Information Technology Management Structure and Governance Framework (OMB Memorandum 09-02):* Reaffirmed and clarified the organizational, functional and operational governance framework required within the Executive Branch for managing and optimizing the effective use of IT.

2009 – *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (OMB Memorandum 09-29): Provided direction to agencies for meeting FY 2009 FISMA reporting requirements.*

2009 – *Update on the Trusted Internet Connections Initiative (OMB Memorandum 09-32):* Provided an overview of the Trusted Internet Connection (TIC) initiative and to request updates to agencies' Plans of Action and Milestones (POA&Ms) for meeting TIC requirements.

2010 – *Open Government Directive (OMB Memorandum 10-06):* Directs executive departments and agencies to take specific action to implement the principles of transparency, participation, and collaboration set forth in the President's Memorandum on Transparency and Open Government.

2010 – *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (OMB Memorandum 10-15):* Provided direction to agencies for meeting FY 2010 FISMA reporting requirements.

2010 – *Guidance for Agency Use of Third-Party Websites and Applications (OMB Memorandum 10-23):* Requires federal agencies to take steps to protect individual privacy whenever using third-party websites and application to engage with the public.

2010 – *Reforming the Federal Government's Effort to Management Information Technology Projects (OMB Memorandum 10-25):* Directed the Federal Chief Information Officer (CIO) to review high-risk IT projects, executive departments and agencies to refrain from awarding task orders or contracts for financial system modernization projects, and OMB's Deputy Director Management to develop recommendation for improving the federal government's IT procurement and management practices.

2010 – *Information Technology Investment Baseline Management Policy (OMB Memorandum 10-27):* Provided policy direction regarding development of agency IT investment1 baseline management policies and defines a common structure for IT investment baseline management policy with the goal of improving transparency, performance management, and effective investment oversight.

2010 – *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS) (OMB Memorandum 10-28):* Outlined and clarified the respective responsibilities and activities of the Office of Management and Budget (OMB), the Cybersecurity Coordinator, and DHS, in particular with respect to the Federal Government's implementation of the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. §§ 3541-3549).

2010 – *NARA Bulletin 2010-05 - Guidance on Managing Records in Cloud Computing Environments:* Addressed records management considerations in cloud computing environments and is a formal articulation of NARA's view of agencies' records management responsibilities.

Table 1.2 Timeline of Major Federal IT Policy (*continued*)

2011 – *Sharing Data While Protecting Privacy (OMB Memorandum 11-02): Encouraged federal agencies to share high-value data, while at the same time reinforcing their responsibility for protecting individual privacy.*

2011 – *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors (OMB Memorandum 11-11):* Outlined DHS's plan of action for agencies that will expedite the Executive Branch's full use of the PIV credentials for access to federal facilities and information systems.

2011 – *Presidential Memorandum Managing Government Records:* Executive branch wide effort to reform records management policies and practices to develop a 21st-century framework for the management of Government records.

2011 – *Delivering on the Accountable Government Initiative and Implementing the GPRA Modernization Act of 2010 (OMB Memorandum 11-17):* Provide interim guidance on implementing the GPRA Modernization Act of 2010.

2011 – *Implementing the Telework Enhancement Act of 2010 IT Purchasing Requirements (OMB Memorandum 11-20):* Provide guidance to ensure the adequacy of information and security protections for information and information system used while teleworking.

2011 – *Implementing the Telework Enhancement Act of 2010: Security Guidelines (OMB Memorandum 11-27):* Provide guidance on security requirements for implementing the Telework Enhancement Act of 2010.

2011 – *Chief Information Officer Authorities (OMB Memorandum 11-29):* Clarifies the primary area of responsibility for Agency CIOs.

2011 – *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (OMB Memorandum 11-33):* Provided direction to agencies for meeting FY 2011 FISMA reporting requirements.

2011 – *Security Authorization of Information Systems in Cloud Computing Environments: Established a federal policy for the protection of federal information in cloud services.*

2012 – *Principles for Federal Engagement in Standards Activities to Address National Priorities (OMB Memorandum 12-08):* Principles and directions to federal agencies in a convening or active engagement with private sector standardization organizations to address national priorities.

2012 – *Implementing PortfolioStat (OMB Memorandum 12-10):* Provided federal agencies with instructions on implementing PortfolioStat reviews.

2012 – *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (DHS FISM 12-02):* Provided direction to agencies for meeting FY 2012 FISMA reporting requirements.

2012 – *Managing Government Records Directive (OMB Memorandum 12-18):*Creates a robust records management framework that complies with statutes and regulations to achieve the benefits outlined in the Presidential Memorandum to reform records management policies and practices to develop a 21st-century framework for the management of Government records.

2012 – *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (OMB Memorandum 12-20): Provided direction to agencies for meeting FY 2012 FISMA reporting requirements.*

Agency CIO.[39] In addition to the decisions of IT procurement, the Agency CIO was required to establish goals and report on efforts to reduce costs and increase efficiency through improved information management [9]. In 2011,[40] the role of the Agency CIO was further expanded to include four additional areas: governance (IT investment review and portfolio management), commodity IT (IT infrastructure, enterprise-wide IT systems, and business support systems), program management (IT program management resource identification, and hiring), and information security (direct or delegated authority and primary responsibility). The Federal CIO Council[41] was also established in 1996[42] to provide a central focal point for coordinating issues across the federal government and to make recommendations for IT management policies.

Today, multiple federal laws and government-wide policies provide the foundation for the federal IT policy framework used to manage and control IT issues within the federal government. The IT policy framework consists primarily of four main sources:

1. Federal statutes, written and enacted by Congress to address major IT issues;
2. Government-wide executive directives and mandates issued by the Office of Management and Budget (OMB) to guide implementation of federal statutes;
3. Department or agency IT-level policies that address department or agency-specific needs and requirements; and
4. IT policies that reflect the requirements of a specific community of interest (COI).[43]

Through this policy framework the government-wide governance manages IT-related issues such as information security, capital planning and investment management, IT strategic planning, enterprise architecture, privacy, records management and retention, and information use (e.g., dissemination, collection, and disclosure).

[39] From Seifert, J. *Government Information Technology (IT) Management: The Clinger-Cohen Act and the Homeland Security Act of 2002*. Washington, DC: The Library of Congress, Congressional Research Service (CRS) Office; 2005. "*The duties of the CIO as described in the act are to provide information management advice and policy to the agency head; develop, maintain, and facilitate information systems; and evaluate, assess, and report to the agency head on the progress made developing agency information technology systems.*"

[40] Office of Management and Budget (OMB) Memorandum 11-29, "*Chief Information Officer Authorities* " was designed to enable Agency CIO to have a direct authority to effectively implement the 25 Point Implementation Plan to Reform Federal IT Management.

[41] From Federal Chief Information Officers Council. About the Council [Internet]. Washington, DC: Office of Management and Budget [cited 2011 September 22]. Available from: http://www.cio.gov/council-about.cfm/csec/1. "*The CIO Council is one element of an interagency support structure established to achieve information resource management objectives delineated in legislation including the E-Government Act of 2002, Government Paperwork Elimination Act, Government Performance and Results Act, and the Information Technology Management Reform Act of 1996.*"

[42] Executive Order 13011, "*Federal Information Technology,* " which became law through the E-Government Act of 2002. Available from: http://csrc.nist.gov/groups/SMA/fasp/documents/personnel security/opmpolicybsp/federal_it_jul_1996.html.

[43] For example, the Committee on National Security Systems (CNSS) establishes policies and directives for the National Security Community.

CLOUD COMPUTING: DRIVERS IN FEDERAL IT TRANSFORMATION

The federal IT environment is transforming. As discussed previously, the *Cloud Strategy* set forth the strategic direction for approaching the adoption of cloud services. However for this cloud transformation to be successful and long-lasting, cultural changes will need to occur to overcome potential resistance of cloud adoption due to obstacles and to establish mitigations to address security and privacy concerns and other challenges that impede[44] the realization of the benefits of cloud solutions. The institution of the federal government's culture towards IT needs to be oriented to considering IT as a service. Through a collaborative partnership between the federal government and industry, the investment in changing individual federal agency business processes will serve as an accelerator in the transformational drivers to improve federal IT. In addition to a change in mindset, Agency CIOs responsible for developing IT strategic plans need to be cultivated to think of cloud services as increasing the efficiency and effectiveness that enable them to address their strategic objectives, goals, and performance measures.

WARNING

One can easily justify how cloud services, if appropriately planned and integrated, could present potential benefits for cost-savings and improve federal IT by maximizing efficiency, improving agility, and enabling innovation. Through the right mixture of cloud computing services, the federal government's IT investment portfolios can achieve better optimization. However, the adoption of cloud computing technologies will likely face ongoing impediments[45] as "there continues to be a need for a more thorough understanding of the cloud's deployment models, unique security implications, and data management challenges" [10]. Example impediments could include:

- Cultural resistance.
- Security and privacy concerns.
- Network access, availability, and resiliency limitations.
- Data portability and standardization.
- Liability and regulations.

Therefore, federal agencies will continue to carefully navigate these challenges to ensure there is a limited impact to their mission and business.

[44] From Badger, L., Bernstein, D., Bohn, R., de Vaulx, F., Hogan, M., Mao, J., et al. NIST Special Publication (SP) 500-293 (Draft) US Government Cloud Computing Technology Roadmap, Volume I Release 1.0. Maryland: National Institute of Standards and Technology; 2011. *The US Government Cloud Computing Technology Roadmap was developed to foster adoption of cloud computing, improving information made available to decision makers, and facilitate development in the cloud computing model.*

[45] "*Challenging Security Requirements for USG Cloud Computing Adoption.*" Available from: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Requirements_for_US_Government_Cloud_Computing_Adoption_v3.3-final.pdf.

Drivers for Adoption

Before proceeding with a discussion of the potential benefits offered to the federal government through the use of cloud computing, it is essential that we gain some basic understanding of some of the possible drivers for cloud adoption. As previously highlighted, the *Cloud Strategy* characterized the federal government's IT environment as: *low asset utilization*, *fragmented demand and duplicative systems*, *environments which are difficult to manage*, and *long procurement lead times* [1]. This characterization was largely the result of the way the federal government has acquired and operated over the years in independent silos.[46] "Federal IT change efforts are typically managed in isolation from business operations, so those working on long-term solutions are too often not concerned with, or even aware of, the evolution of day-to-day business considerations" [11]. These silos have led to the continued decentralization of the federal IT environment, mostly because the federal agencies have developed overlapping, duplicative, and, in many instances, fragmented programs that are not always shared across the federal government or community boundaries. However, these are not necessarily new issues. The scope of federal IT may have changed (i.e., size and complexity of programs, services, and systems), but

NOTE

- In May 2002, OMB identified ten potentially redundant systems across the federal government that related to the rule making process.[47] As a result, OMB focused on "consolidating redundant IT systems relating to the President's on-line rulemaking initiative" [12].
- The GAO reported in May 2004, "the duplicative and stovepiped nature of DOD's [US Department of Defense] systems environment is illustrated by the numerous systems it has in the same functional areas. For example, DOD reported that it has over 200 inventory systems. These systems are not integrated and thus have multiple points of data entry, which can result in data integrity problems" [13].
- In a March 2011 GAO report, "Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue," the GAO "identified 81 areas for consideration—34 areas of potential duplication, overlap, or fragmentation as well as 47 additional cost-saving and revenue-enhancing areas" [14]. Although not all specifically related to the duplication of IT resources, since IT plays a critical role in supporting most government programs and mission-specific operations, many areas of duplication would include the underlying IT capabilities.

[46] A self-contained organizational structure that can operate independent of others within the larger organization.

[47] Executive Office of the President, Office of Management and Budget. Regulation Information Frequently Asked Questions [cited 2011 Jul 27]. Available from: http://www.reginfo.gov/public/jsp/Utilities/faq.jsp. *Federal regulations are created through a process known as "rulemaking," which is governed by the Administrative Procedure Act (APA) (5 U.S.C. Chapter 5).*

NOTE

On January 14, 2010, the White House held "*The Forum on Modernizing Government*" where the forum noted the following conclusion:

> *The Federal Government has difficulty managing large-scale technology efforts. The Forum made it clear that there are best practices in industry for the design and ongoing review of these types of technology efforts that increase their likelihood of success. By comparison to these industry best practices, most Federal Government IT projects are too large and not sufficiently integrated into business unit operations. Multi-year Federal IT efforts are typically driven by technology managers—who often turn over during the life of the project—rather than agency business leaders. Agency business leaders are not held accountable for project success, and in turn do not adequately invest in IT project management. As a result, in comparison to industry best practices, Federal IT projects are too often marked by milestones spaced too far apart and deliverables that fail to deliver tangible end-user value [16].*

NOTE

It is important to note, the challenges within the federal IT were not created overnight. GAO, OMB, and other organizations within the federal government have repeatedly highlighted weaknesses in required federal IT processes and controls to address IT reform challenges, and the ineffective government-wide and federal-agency-specific IT oversight and management. As early as 2000, the GAO highlighted OMB's role as being "responsible for providing direction on government-wide information resources and technology management and overseeing agency activities in these areas, including analyzing major agency information technology investments" [18]. Although not limiting the governance over IT investments within each federal agency, a central focal point was noted as lacking to serve as this catalyst, working in conjunction with other executive officials to ensure that information resources and technology management issues were addressed within the context of the government's highest priorities and not in isolation from them [18].

the lack of strategic alignment and functional integration[48] between federal agencies has existed long before the *Cloud Strategy*. This misalignment has led to expensive and overly redundant development and maintenance costs. Across the federal government, multiple instances of similar shared services[49] have been developed, IT

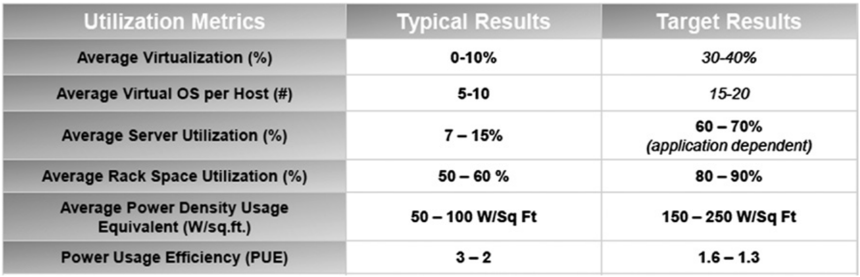
[48] From Office of Management and Budget (OMB). The Common Approach to Federal Enterprise Architecture. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. *"Functional integration means interoperability between programs, systems, and services, which requires a meta-context and standards to be successful."*

[49] From VanRoekel, S. *Federal Information Technology Shared Services Strategy*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. *"The Federal Information Technology Shared Services Strategy provides organizations in the Executive Branch of the United States Federal Government (Federal Agencies) with policy guidance on the full range and lifecycle of intra- and inter-agency information technology (IT) shared services, which enable mission, administrative, and infrastructure-related IT functions."*

modernization efforts have been independently executed, and information security programs have been operated with little or no intra- and inter-agency coordination.

The duplication, coupled with the low utilization of IT resources, has continued to increase federal IT costs. Federal agencies (and even program management offices) have worked independently to procure new hardware to satisfy their need for additional capacity, rather than optimizing the existing IT resources, either across an agency or between multiple agencies (for multi-agency programs). As an example, in 2010, as an output of the initial findings of the Federal Data Center Consolidation Initiative (FDCCI),[50] average server utilization rates were noted as low as 7% [15]. The absence of an effective IT management structure within the federal government has led to this underutilization of computing and storage resources. In the course of the initial phases of the FDCCI project, metrics similar to those included in Figure 1.5 were established to assist federal agencies in making more informed IT management decisions for improving utilization within their consolidation plans.[51]

Another potential driver that is related to adoption of cloud computing includes issues associated with the IT acquisition process. Federal IT acquisition has been stagnant and largely unchanged for years. For example, in 1995, the GAO conducted a statistical analysis of the time taken to complete an IT acquisition, and noted that the time can vary depending on the dollar value, procurement type, and whether a bid protest was filed [17]. These same challenges still exist today.



Utilization Metrics	Typical Results	Target Results
Average Virtualization (%)	0-10%	*30-40%*
Average Virtual OS per Host (#)	5-10	*15-20*
Average Server Utilization (%)	7 – 15%	60 – 70% *(application dependent)*
Average Rack Space Utilization (%)	50 – 60 %	80 – 90%
Average Power Density Usage Equivalent (W/sq.ft.)	50 – 100 W/Sq Ft	150 – 250 W/Sq Ft
Power Usage Efficiency (PUE)	3 – 2	1.6 – 1.3

FIGURE 1.5 Example FDCCI Utilization Metrics [15]

[50] From Kundra, V. *The Federal Data Center Consolidation Initiative*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. *"The FDCCI seeks to curb this unsustainable increase in the number of data centers by reducing the cost of data center hardware, software, and operations; shifting IT investments to more efficient computing platforms; promoting the use of Green IT by reducing the overall energy and real estate footprint of government data centers; and increasing the IT security posture of the government."*

[51] FDCCI Data Center Consolidation Plans. Available from: http://www.cio.gov/pages.cfm/page/FDCCI-Public-Plan-Links.

The continued delays in streamlining the acquisition process have limited the potential benefits in the investment of IT. However, streamlining the acquisition process is not enough. Federal agencies will need to make improvements in their federal IT management practices to learn how to effectively leverage the cost-savings provided by technologies such as virtualization and cloud computing and make changes to their practices to accommodate acquiring IT as a Service.[52]

Cloud Benefits

The *Cloud Strategy* offered the following key benefits to improved operational *efficiency, agility, and innovation* through the use of cloud computing.

- *Efficiency*—better use of existing resources through a service-based model with a focus on improving utilization and to use technologies that would reduce duplicative services across the federal government.
- *Agility*—ability to deliver service faster and provision new resources based on the federal agencies' prioritization. For example, existing services that require long lead times to upgrade or increase/decrease capacity would receive high priority over services that are easier to upgrade, not sensitive to demand fluctuations, or unlikely to need upgrade in the longer term [19].
- *Innovation*—more access to innovation delivered through private sector services.

A summarization of the benefits provided in Table 1.3 describes how different characteristics of the federal IT environment can be improved through cloud adoption. Through these improvements, the *Cloud Strategy* suggested federal agencies could benefit because they could redirect their "focus on mission-critical tasks instead of purchasing, configuring and maintaining redundant infrastructure" [19].

The 25 Point Implementation Plan to Reform Federal Information Technology Management highlighted similar benefits offered through the adoption of cloud computing, through a service-based model as:

- *Economical:* Pay-as-you go approach to IT offers a lower initial investment, while allowing the ability to add investments as system usage increases [19].
- *Flexible:* Fluctuations in user demand and capacity can be added or subtracted without acquiring additional hardware and software [19].
- *Fast:* Long procurement times can be eliminated, while also enabling access to a continuously growing selection of services [19].

[52] In February 2012, the Federal CIO Council and the Chief Acquisition Officers Council in coordination with the Federal Cloud Compliance Committee published the best practices to assist federal agencies in acquiring cloud services. Available from: http://www.cio.gov/cloudbestpractices.pdf.

Table 1.3 Cloud Benefits: Efficiency, Agility, Innovation [19]

Cloud Benefits	Current Environment
Efficiency	
• Improved asset utilization (server utilization > 60–70%) • Aggregated demand and accelerated system consolidation (e.g., Federal Data Center Consolidation Initiative) • Improved productivity in application development, application management, network, and end-user	• Low asset utilization (server utilization < 30% typical) • Fragmented demand and duplicative systems • Difficult-to-manage systems
Agility	
• Purchase “as-a-service” from trusted cloud providers • Near-instantaneous increases and reductions in capacity • More responsive to urgent agency needs	• Years required to build data centers for new services • Months required to increase capacity of existing services
Innovation	
• Shift focus from asset ownership to service management • Tap into private-sector innovation • Encourages entrepreneurial culture • Better linked to emerging technologies (e.g., devices)	• Burdened by asset management • De-coupled from private-sector innovation engines • Risk-adverse culture

However, to achieve sustainable benefits, the federal government will require more than just adopting new services and technologies. Federal stakeholders will need to commit to long-term transformational change in both the federal IT environment and culture.

Cloud computing reinvents the federal government’s IT business model, from capital expenditures (CAPEX) to operational expenditures (OPEX). With any significant change in business operations, there is an upfront cost required to support IT transformation. Federal agencies will need to understand that these costs may not be recaptured immediately, and will likely have to wait months, if not years, before savings are fully realized. Therefore, the benefits previously described will need to be weighed against the maturity of current federal IT processes and practices already established to determine if changes need to be made. Federal agencies will need to ensure the transformation benefits match their expectation of improved operational efficiency, resource optimization (e.g., data center real estate, compute, storage, etc.), and increased security through the delivery of IT as a service, something that will require change in the way the federal government plans for IT.

Improving Efficiency

The transition to cloud services is more than a change in technology delivery models. It is also a shift in the focus from a federal government driven by IT asset ownership to service management. By exploiting the benefits of on-demand resource provisioning, federal agencies can learn to better understand their capacity requirements by scaling their usage, thereby improving overall utilization. Compared to fragmented and duplicative IT environments created by the investment in heterogeneous infrastructures in data centers across the country and around the world, the federal government can leverage cloud computing capability as a means to enable them to efficiently consolidate, transitioning the total cost of ownership (TCO) of data centers and offering the ability to repurpose the savings to support their mission and business.

Improving Agility

Agility in cloud computing provides federal agencies with the capability to rapidly provision/de-provision resources (e.g., compute, storage) as changes occur in their business requirements, making them more responsive and provides an opportunity to focus on identifying sources for improving their overall agency performance.[53]

Improving Innovation

Federal agencies have operated in a mode that has focused on avoidance of risk, rather than managing risk. This has largely kept the federal government from innovating at a pace similar to the private sector. Cloud adoption will enable federal agencies to become more innovative through better service delivery by leveraging existing cloud services and emerging technologies that would increase their operational effectiveness.

DECISION FRAMEWORK FOR CLOUD MIGRATION

The *Cloud Strategy* presented a three-step structured framework. As depicted in Table 1.4, federal agencies can use the tool for assisting them when considering the migration to cloud services. As previously discussed, cloud transformation requires a shift in mindset. Federal agencies have been cultured to manage assets because it enables them to have more control over their IT infrastructure. The shift in mindset to managing IT as a service will require federal agencies to rely more on CSPs, a significant first challenge to overcome in cloud transformation.

[53] The Government Performance and Results Act (GPRA) Modernization Act of 2010 (GPRAMA) focuses improving performance and management to include information technology. Available from: www.gpo.gov/fdsys/pkg/PLAW ... /PLAW-111publ352.pdf.

Table 1.4 Decision Framework for Cloud Migration [1]

Select	Provision	Manage
• Identify which IT services to move and when – Identify sources of value for cloud migrations: efficiency, agility, innovation – Determine cloud readiness: security, market availability, government readiness, and technology lifecycle	• Aggregate demand at department level where possible • Ensure interoperability and integration with IT portfolio • Contract effectively to ensure agency needs are met • Realize value by repurposing or decommissioning legacy assets and redeploying freed resources	• Shift IT mindset from assets to services • Build new skill sets as required • Actively monitor SLAs to ensure compliance and continuous improvement • Re-evaluate vendor and service models periodically to maximize benefits and minimize risks
Framework is flexible and can be adjusted to meet individual agency needs.		

Throughout the remainder of this section, we will briefly discuss each of the steps in the decision framework to demonstrate how they can be applied to a "Federal Agency" (*a generic reference to a federal agency cloud service customer*).[54]

Selecting Services to Move to the Cloud

First the "Federal Agency" needs to decide if it is ready to migrate to the cloud. In addition to the "Federal Agency" readiness, the *Cloud Strategy* identified several factors when performing a risk-based[55] evaluation of the readiness of CSPs as a preliminary activity to considering cloud services such as *security requirements*, *service characteristics*, *market characteristics*, *network infrastructure*, *application and data, government readiness*, and *technology lifecycle* [1]. After the "Federal Agency" has decided it is ready to migrate some of its services to the cloud, the next

[54] As an example, in May of 2012, the Federal Aviation Administration (FAA) released the FAA Cloud Computing Strategy. Available from: http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/atc_comms_services/swim/documentation/media/cloud_computing/FAA%20Cloud%20Computing%20Strategy%20v1.0.pdf.

[55] The European Network and Information Security Agency (ENISA) published the *Security and Resilience in Government Clouds* that provides decision-making model for the identification of cloud solutions that meet the organization requirements. Available from: http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds.

important question is: "What services to move?" This determination calls for a full understanding of its IT investment portfolio and risk tolerance, among other things. Preliminary activities may include the "Federal Agency" CIO in collaboration with other key stakeholders to establish a clear set of criteria that will be used as a part of evaluating CSPs. Part of this process may include "identifying security, privacy, or other requirements for cloud services to meet, as a criterion for the selection of a cloud provider" [20].

Next, the "Federal Agency" should conduct a full evaluation of the current IT portfolio for potential services that are candidates to be included in its cloud adoption roadmap and plans. The services might be prioritized based on the "expected values" and "cloud readiness." Since the federal government tends to operate with a predominately risk-adverse mindset, the "Federal Agency" may need to develop additional metrics. These metrics could be used to measure the expected value by the "Federal Agency," and the readiness of both the "Federal Agency" and CSPs (commercial or federal government). By evaluating short- and long-term benefits (i.e., efficiency, agility, and innovation) the "Federal Agency" can seek to properly align its migration planning with its governance and risk management functions that place an emphasis on identifying mitigations that would assist the "Federal Agency" in minimizing potential risks during the migration process.

Provisioning Cloud Services Effectively

The federal government has had a history of "IT outsourcing." However, most IT outsourcing has been conducted by a "single" federal agency or multiple federal agencies through a joint program management office (PMO) using traditional procurement methods to contract services from providers to build and host services, applications, and information. In these types of outsourcing arrangements, the federal government mostly maintained control over IT assets and their information. By purchasing IT "on-demand," unique requirements may arise that federal agencies will need to address when contracting with CSPs [21]. Therefore, provisioning cloud services will require a change in the "Federal Agency" acquisition processes and practices. This new model of provisioning IT service will also enable the "Federal Agency" to be more cost-effective by pooling together the purchasing power through an aggregation of demand to the greatest extent possible before migrating services to the cloud [1].

Additionally, the *Cloud Strategy* outlined several other considerations [1] the "Federal Agency" should consider to reduce the risk associated with migrating to the cloud and to maximize efficiency such as:

- Integration of the IT service into the IT portfolio and functions that support business processes.
- Effective implementation of contract provisions that ensure portability and encourage competition (limit vendor lock-in); explicitly include service level agreements (SLAs) for security, continuity of operations, and service quality

based on specific agency needs; and specific metrics that clearly state how and when they will be collected.

- Realizing the value through the appropriate use of cloud services through the decommissioning and release of assets used to support legacy applications and servers.

Managing Services Rather Than Assets

When the "Federal Agency" has successfully migrated to the cloud, differences may exist in the relationship between the "Federal Agency" and the CSP, which will require adopting new governance processes. The "Federal Agency" will need to ensure it can effectively manage SLAs based on the metrics defined previously as part of cloud service selection activity. "SLAs should clearly define how performance is guaranteed (such as response time resolution/mitigation time, availability, etc.) and require CSPs to monitor their service levels, provide timely notification of a failure to meet the SLAs, and evidence that problems have been resolved or mitigated" [21]. SLA monitoring will also require the "Federal Agency" to actively evaluate the metrics to ensure they are enforced and usage charges are accurate. Since portability, interoperability, and security are key requirements for cloud service selection, the "Federal Agency" can periodically re-evaluate the market to identify opportunities that maximize capabilities offered by changes in technologies, new cloud services, and private-sector innovations.

SUMMARY

In this chapter a brief overview of the *Cloud Strategy* was presented to highlight the key drivers for the federal government's adoption of cloud computing. In addition, the introduction provides CSPs with a basic understanding of how the strategy may be used by federal agencies considering cloud services as an extension of their IT portfolio. We briefly reviewed the history of federal IT with the purpose of understanding the potential challenges that may be a force behind the cloud adoption. We also discussed the key drivers for federal IT transformation and the expected benefits received through cloud computing. Lastly, a brief examination of the three-step decision framework offered insight into its application for cloud migration.

References

[1] Kundra V. Federal cloud computing strategy. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011.

[2] US Congress, Office of Technology Assessment (OTA). Federal government information technology: management, security, and congressional oversight. Washington: US Government Printing Office; 1986.

[3] Paperwork Reduction Act [Internet]. Washington: US National Archives and Records Administration [cited July 7, 2012]. <http://www.archives.gov/federal-register/laws/paperwork-reduction/3504.html>.

[4] Melvin V. Federal chief information officers: opportunities exist to improve role in information technology management. Washington: US Government Accountability Office; 2011.

[5] Comptroller General of the United States. Acquisition and use of software products for automated data processing systems in the federal government. Washington: US General Accounting Office; 1971.

[6] Staats EB. Uses of minicomputers in the federal government: trends, benefits, and problems. Washington: US General Accounting Office; 1976.

[7] Finch JC. Use of Minicomputers for Internal Revenue Service Tax Return Preparation. Washington: US General Accounting Office; 1978.

[8] Comptroller General of the United States. Problems found with government acquisition and use of computers from November 1965 to December 1976. Washington: US General Accounting Office; 1977.

[9] Seifert J. Government information technology management: past and future issues (The Clinger-Cohen Act). Washington, DC: The Library of Congress, Congressional Research Service (CRS) Office; 2002.

[10] McClure D. Statement of Dr. David McClure, Associate Administrator, Office of Citizen Services and Innovative Technologies, US General Services Administration, Before the House Science, Space and Technology Committee, Subcommittee on Technology and Innovation. Washington: US House of Representatives; 2011.

[11] Office of Management and Budget (OMB). White House forum on modernizing government: overview and next steps. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.

[12] Daniels ME. Office of Management and Budget (OMB) Memorandum 02-08, Redundant Information Systems Relating to On-Line Rulemaking Initiative. Washington, DC: Executive Office of the President, Office of Management and Budget; 2002.

[13] Katz GD, Rhodes KA. DOD business systems modernization: billions continue to be invested with inadequate management oversight and accountability. Washington: US General Accounting Office; 2004.

[14] Dodaro GL. Opportunities to Reduce Potential Duplication in Government programs, Save Tax Dollars, and Enhance Revenue. Washington: US Government Accountability Office; 2011.

[15] Federal Data Center Consolidation Initiative (FDCCI). Workshop III: Final data center consolidation plan [Internet]. Washington: US General Services Administration [cited July 18, 2011]. <http://www.cio.gov/documents/FDCCI%20Workshop%20III%20%20Aug%2010th%20010.pdf13>.

[16] White House. White House forum on modernizing government: overview and next steps. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.

[17] Brock JL. Information Technology: A Statistical Study of Acquisition Time. Washington: US General Accounting Office; 1995.

[18] McClure DL. Leadership Needed to Confront Serious Challenges and Emerging Issues. Washington: US General Accounting Office; 2000.

[19] Kundra V. 25 Point implementation plan to reform federal information technology management. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.

[20] Jansen W, Grance T. NIST Special Publication (SP) 800-144, guidelines on security and privacy in public cloud computing. Maryland: National Institute of Standards and Technology; 2011.

[21] Federal CIO Council and Chief Acquisition Officers Council. Creating effective cloud computing contracts for the federal government. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012.

CHAPTER

Cloud Computing Standards 2

INFORMATION IN THIS CHAPTER:

- Introduction
- Standards Development Primer
- Cloud Computing Standardization Drivers
- Identifying Standards for Federal Cloud Computing Adoption

INTRODUCTION

Standardization can be characterized as the process by which new standards are developed or new products are brought to market implementing standards. A standard (or technical standard) can be classified differently and published by many different organizations. In Table 2.1 the generally accepted definitions are provided for what constitutes a standard for use by the US government.

Standards play a critical role for cloud adoption, both by the federal government[1] and the private sector. As we will discuss later in this chapter, the federal government has a unique responsibility to ensure *voluntary consensus standards* are adopted in lieu of *government-unique standards.*

The *Federal Cloud Computing Strategy* identified the importance of standards development to ensure the federal government's adoption and effective use of cloud computing and related technologies is supported by broad standardization. For federal agencies to leverage the capabilities and achieve the benefits offered by cloud computing, as described Chapter 1, the development of standards will need to focus

[1] From Kundra, V. *Federal Cloud Computing Strategy.* Washington: Executive Office of the President, Office of Management and Budget; 2011. *"Standards encourage competition by making applications portable across providers, allowing Federal agencies to shift services between providers to take advantage of cost efficiency improvements or innovative new product functionality."*

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00002-2

Table 2.1 Sources of the US Government Definition of Standard

Source	Definition
National Institute of Standards and Technology (NIST) Cloud Computing Standards Roadmap	"a document, established by consensus and approved by a recognized body that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context" [1]
Office of Management and Budget (OMB) Circular No. A-119, Revised codified in National Technology Transfer and Advancement Act (NTTAA)	"common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods, and related management systems practices" [2] "the definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength" [2]

on three major areas[2]: *interoperability*,[3] *portability*,[4] and *security*.[5] For example, standards "ensure clouds have an interoperable platform so that services provided by different providers can work together, regardless of whether they are provided using public, private, community, or a hybrid delivery model" [3].

To support the interests of the federal government, NIST was charged with providing technical guidance and support in the standards development efforts relating to cloud computing. The NIST Cloud Computing Program,[6] through the Cloud Computing Standards Roadmap Working Group,[7] focused on the development and maintenance of a Cloud Computing Standards Roadmap[8] that bolstered the federal government's ability to adopt cloud computing. In addition, NIST was also responsible for directing and managing the strategic and tactical programs to ensure standards that already existed or are in development are integrated into the US

[2] The first edition of the NIST Cloud Computing Standards identified expanded consideration in other areas such as maintainability, usability, reliability, and resiliency.

[3] Examples include functional and management service interfaces.

[4] Examples include workloads, storage, and data.

[5] Examples include authentication, data security, identity and access management, encryption and key management, governance, and compliance.

[6] In 2010 the NIST Cloud Computing Program was launched at the direction of Vivek Kundra, the former US Federal CIO.

[7] *NIST Cloud Computing Standards Roadmap Working Group*. Available from: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsRoadmap.

[8] *NIST Cloud Computing Standards Roadmap*. Available from: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf.

government's Cloud Computing Technology Roadmap.[9] For the roadmap to be successful, NIST's participation was important to ensure standards development supported acceleration by the private sector that would implement those new standards in products and services that could be procured by federal agencies.

Cloud computing is supported by many existing and emerging standards. Although not all of them were specifically developed with cloud computing in mind, many of them do directly support cloud services delivery. NIST and many leading industry groups and associations[10] have focused on identifying the technology standards gaps for the development of cloud-specific standards, including broad standardization. When a significant gap within standards exists, standards organizations, industry groups, and the cloud communities are faced with the challenge of coordinating their efforts to ensure interoperability between standards and to limit the impact associated with too many standards.[11] For example, overlapping and duplicative standards efforts may attempt to solve the same problem, inadvertently causing competition for the "best" standard to fill the gaps. Therefore, standards convergence is important to ensure standards are developed to address the need for compatibility.

NOTE

NIST [4] defined Cloud Computing Deployment Models as:

- *Private cloud*—the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- *Community cloud*—the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- *Public cloud*—the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- *Hybrid cloud*—the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

[9] *NIST Cloud Computing Program.* Available from: http://www.nist.gov/itl/cloud/.

[10] For example, Distributed Management Task Force, Inc. (DMTF), Open Grid Forum (OGF), and Storage Networking Industry Association (SNIA).

[11] *Cloud Computing Standards: Too Many Cooks in the Kichen?* Available from: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/ForumVAgenda.

STANDARDS DEVELOPMENT PRIMER

Standards development organizations (SDOs) typically have a process they follow for developing standards. As an example, the International Organization for Standardization (ISO)[12] follows a six-step standards development process[13] that includes: *proposal*, *preparatory*, *committee*, *enquiry*, *approval*, and *publication*. In Figure 2.1, the NIST Cloud Computing Standards Roadmap provided a "high-level conceptualization of how IT standards are developed and standards-based IT products, processes, and services are deployed" [1]. Although only exemplary, the lifecycle does offer a useful reference to understand the workflow within the standards development process as it relates to standards maturity and market adoption into products and services.

The US standardization system is based on a set of globally accepted principles for standards development [5]. Voluntary consensus is a critical part of this standardization system. A consensus-based process ensures standards meet the needs of both public and private sector[14] stakeholders before being finalized. The federal government's adoption of standards needs to be consistent with the objectives of the Technical Barrier to Trade (TBT)[15] Committee. By leveraging an "international" focused set of principles such as transparency, openness, and consensus, the federal government can ensure that standards development increases the likelihood of standardization in cloud computing.

As standards mature and broader market acceptance begins to see more participants, an emphasis will need to be placed on ensuring products and services are conforming to the standards and requirements for implementation. Therefore, standardization requires a process known as *conformity assessment*, to demonstrate "that products, processes, systems, services or personnel fulfill the requirements that are identified in a specified standard. Conformity assessment forms a vital link between standards that define product characteristics or requirements and the products themselves" [5].

The conformity assessment process provides both the federal government and industry with the confidence that a Cloud Service Provider (CSP) has implemented standards that meet the interoperability, portability, and security requirements necessary to maximize the benefit offered by cloud computing. It also provides a

[12] ISO Stages of the development of International Standards, ISO/IEC Directives, Part 1, *Consolidated ISO Supplement – Procedures specific to ISO,* Section 2 "Development of International Standards." Available from: http://isotc.iso.org/livelink/livelink?func=ll&objId=4230452&objAction=browse&sort=subtype.

[13] The ISO also has options for fast tracking if a document meets specific criteria for maturity. For more information on the standards development process and procedures, refer to ISO/IEC Directives, Part 1, *Procedures for the technical work*, Annex F "Options for development of a project." http://isotc.iso.org/livelink/livelink?func=ll&objId=4230455&objAction=browse&sort=subtype.

[14] The terms "public sector" and "private sector" are used to identify the difference between government and non-government entities.

[15] From World Trade Organization (WTO) Technical barriers to trade [Internet]. Geneva: World Trade Organization Technical; [cited 2011 September 28]. Available from: http://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm. *"The Agreement on Technical Barriers to Trade tries to ensure that regulations, standards, testing and certification procedures do not create unnecessary obstacles."*

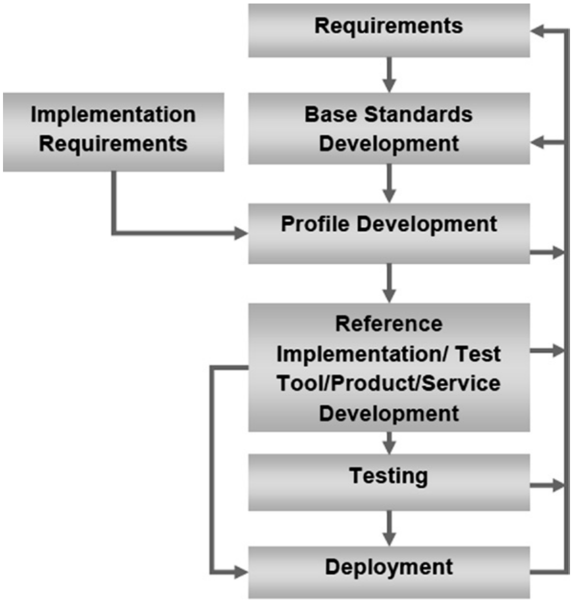

Requirements
Implementation Requirements
Base Standards Development
Profile Development
Reference Implementation/ Test Tool/Product/Service Development
Testing
Deployment

FIGURE 2.1 IT Standards Life Cycle [1]

TIP

Standards adoption is an evolutionary process. Throughout the process, standards grow in both acceptance and maturity, and it could take years for standards to mature. Most standards can be generally classified as one (or more) of the following types at some point within the standards development lifecycle.[16]

- *Open* standards are open to anyone to participate in developing and implementing (e.g., royalty-free).
- *Proprietary* specifications are privately developed and are usually licensed for implementation. Sometimes, although not always, once they receive enough industry acceptance, they evolve into de facto standards.
- *De facto* standards are considered industry norms through broad adoption and "in practice" application. They have gained acceptance and are therefore expected rather than required to be part of a product roadmap.
- *De jure* standards are formalized through a standards body, thereby making them widely approved because of their formal acceptance.

framework for CSPs to use when assessing their own products and services against standards, potentially making them more competitive within industry based on consumer requirements for specific standards.

[16] Sometimes standards maintain their status as either "de facto" or "de jure" throughout their entire lifetime.

CLOUD COMPUTING STANDARDIZATION DRIVERS

The key driver for the federal government in supporting the standardization of cloud solutions is to address security, portability, and interoperability requirements. For example, without commonly implemented standards addressing interoperability and portability, federal agencies may be required to make significant changes to their software or adapt their code to work within a specific cloud service environment through proprietary Application Programming Interfaces (APIs).[17] This potentially could increase the cost of migrating between CSPs, creating a scenario that may become a barrier for a particular federal agency that has a concern about being locked into a specific cloud service.

Many standards used in cloud computing are a convergence of existing standards. As cloud computing technologies mature, consensus within the industry will begin to establish new standards specifically developed for cloud environments. The NIST Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)[18] initiative was established to support the acceleration of adopting these new standards by developing tests that show the extent to which specific use cases can be supported by cloud systems through a set of documented and public cloud system specifications [6].

Federal Laws and Policy

The federal government is directly concerned with setting and implementing standards through legislation, regulation, or contractual obligations for sales to government purchasers [7]. In its roles, supporting standards development accelerates the broader adoption of cloud computing within the federal government and also assists federal agencies in satisfying their responsibility under federal laws and policies. This responsibility requires them to use voluntary consensus standards, where practical, in their procurement activities.

Trade Agreements Act (TAA)

The Trade Agreements Act of 1979 (TAA)[19] governs trade agreements negotiated with other countries. Under the TAA, federal agencies are prohibited from engaging "in any standards-related activity that creates unnecessary obstacles to the foreign commerce of the United States" [8] and are required to consider international standards. However, the TAA also could prohibit data housed in cloud computing servers

[17] Apache LibCloud (http://libcloud.apache.org/) and Deltacloud (http://incubator.apache.org/deltacloud/) are among a few initiative provide API abstractions from incompatible or difference in multiple cloud providers proprietary APIs.

[18] *Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)*. Available from: http://www.nist.gov/itl/cloud/sajacc.cfm.

[19] *Trade Agreements Act of 1979*. Available from: http://uscode.house.gov/download/pls/19C13.txt.

and storage devices reside within the countries[20] not covered under the Act.[21] NIST supports the implementation of the TAA, including educating federal, state, and local governments on the fundamentals of standards, conformity assessment, and technical regulations.

National Technology Transfer and Advancement Act (NTTAA)

The National Technology Transfer and Advancement Act of 1995 (NTTAA) established a requirement that federal agencies use technical standards that are developed or adopted by voluntary consensus standards bodies and participate with such bodies in the development of technical standards [9]. NIST, through the Standards Coordination Office (SCO),[22] directly supported the requirement of the NTTAA by coordinating within the federal government, and state and local governments, the adoption of voluntarily developed standards.

Office of Management and Budget (OMB) Circular A-119

The OMB Circular A-119 "directs agencies to use voluntary consensus standards in lieu of government-unique standards except where inconsistent with law or otherwise impractical" [10]. The circular focused on minimizing the reliance on unique government standards. Consistent with the requirements of OMB Circular A-119, the Federal Cloud Computing Strategy established requirements for a cooperative effort between public and private sector organizations for the development of standards that would enable the federal government to securely adopt cloud computing technologies.

America COMPETES Reauthorization Act of 2010

The America Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science (COMPETES) Act directs NIST to collaborate with industry in the development of standards supporting trusted cloud computing infrastructures, metrics, interoperability, and assurance; and support standards development with the intent of supporting common goals [11]. In addition, the National Science Foundation (NSF) was directed to "support a national research agenda in key areas affected by the increased use of public and private cloud computing" [11].

Adoption Barriers

Cloud computing as defined by NIST is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned

[20] *FAR Subpart 25.4—Trade Agreements*. Available from: https://www.acquisition.gov/far/current/html/Subpart%2025_4.html#wp1086589.

[21] *Data Center Location Requirement—Protest.* Available from: http://www.gao.gov/decisions/bidpro/405296.pdf.

[22] *NIST Standards Coordination Office (SCO)*. Available from: http://www.nist.gov/director/sco/.

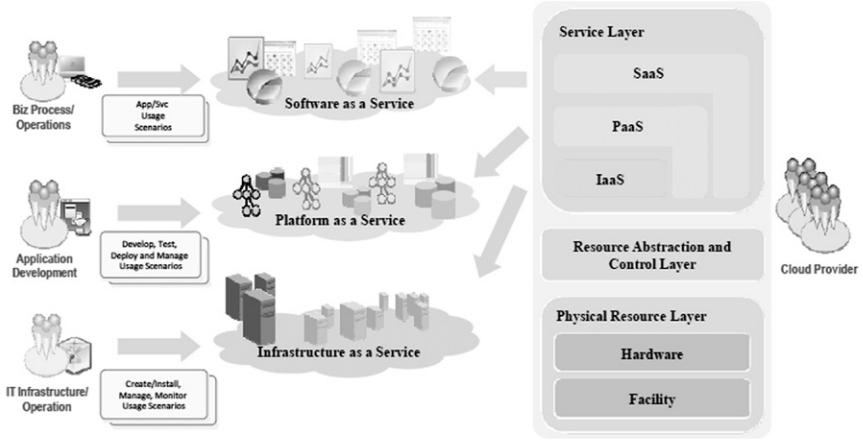


FIGURE 2.2 Cloud Usage Scenarios and Cloud Service Layers [13]

and released with minimal management effort or service provider interaction" [12]. With different cloud deployment and service models available (including derivatives classifications), standards development is an essential part of ensuring the federal agencies' adoption of cloud computing technologies is not hindered by potential barriers such as poorly defined, or a lack of market acceptance of, standards. These barriers limit federal agencies from maximizing their cost-savings through the use of cloud services, impacting their ability to deliver results and produce opportunities for value creation.

As cloud computing matures, open and proprietary standards will co-exist within the cloud computing ecosystem. As illustrated in Figure 2.2, usage scenarios driving Cloud Computing Standards development will be different at each of the service layers (i.e., data portability at the Software as a Service layer and VM portability at the Infrastructure as a Service layer).

The requirements for each of the usage scenarios will need to support well-defined and documented standards or specifications to ensure the federal government's interoperability, portability, and security requirements can be satisfied.

TIP

The Federal Cloud Computing Strategy highlighted the need for federal agencies to consider the market characteristic (i.e., the competitiveness and maturity) for selecting services as part of their decision process for moving to the cloud. The strategy stated that "agencies should consider the availability of technical standards for cloud interfaces which reduce the risk of vendor lock-in" [3]. It also highlighted the important of considering, in addition to security, the interoperability and portability requirements as an aspect to address in the development of contracts to procure cloud services.

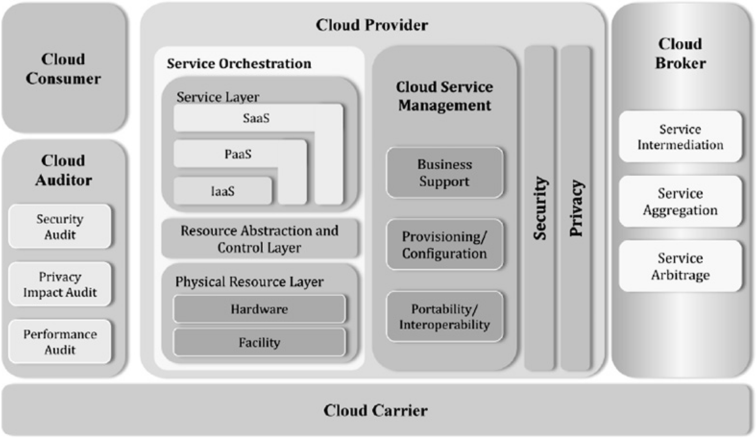


FIGURE 2.3 NIST Conceptual Reference Model [3]

IDENTIFYING STANDARDS FOR FEDERAL CLOUD COMPUTING ADOPTION

The NIST Cloud Computing Reference Architecture Working Group generated a consensus conceptual reference model. The conceptual reference model, illustrated in Figure 2.3, provides a "high-level" model to assist in understanding, discussing, categorizing, and comparing cloud services to communicate and analyze security,[23] interoperability,[24] and portability[25] candidate standards and reference implementations [13].

In addition, the Conceptual Reference Model provides a useful tool for mapping and a common frame of reference for identifying the standards that will be required to facilitate adoption. By understanding the underlying business or technical use cases,[26] specific emphasis can be placed on those areas where gaps in standards exist based on the cross-cutting requirements. Federal agencies, as a cloud computing actor,[27] are the most likely sources for usage scenarios and for identifying requirements.

[23] Examples include authentication and authorization, confidentiality, integrity, and identity and access management.

[24] Examples include the interoperability of services through the service management (consumer APIs) and functional interfaces.

[25] Examples include data and workload portability.

[26] *NIST Cloud Computing Business Use Cases Working Group*. Available from: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/BusinessUseCases#Federal_Business_Use_Cases.

[27] Five actors were identified in the NIST Cloud Computing Reference Architecture: *consumer, provider, auditor, broker,* and *carrier*.

Federal agencies' participation in the standards development process helps in the acceleration of the development and use of Cloud Computing Standards and standards-based products, processes, and services [14].

Standards Development Organizations (SDOs) and Other Community-Driven Organizations

Standards development for cloud computing requires the active involvement of multiple standards bodies. Standards bodies are standards setting organizations that usually consist of stakeholders such as organizations or companies that produce technical standards to address the market's needs for standardization. Table 2.2 lists some of the international and national standards bodies involved in developing cloud computing standards.

Standards Inventory

Standards for cloud computing will continue to evolve, mature, and gain acceptance. This chapter does not attempt to provide a comprehensive catalog of standards supporting cloud computing, as harmonization of standards could take many years. Instead, it attempts to address the importance for cloud standards to promote openness and flexibility of choice by the federal government, while also supporting the minimum requirements of *interoperability*, *portability*, and *security*. This requires a focus on continued development of cloud computing use cases to anticipate where cloud technologies will be used, so that standards organizations, industry groups, and associations can coordinate their efforts to define existing standards, and identify where new standards will need to be developed.

The US Government Cloud Computing Technology Roadmap[28] required the development of a Cloud Computing Standards Roadmap for prioritizing standards developed to support the federal government's interoperability, portability, and security requirements. As part of the Cloud Computing Standards Roadmap development, the NIST Cloud Computing Standards Roadmap Working Group conducted a survey, included in Tables 2.3–2.5, to identify existing industry standards. The results included an inventory of standards that provides a starting point for mapping to

[28] From National Institute of Standards and Technology (NIST). NIST Cloud Computing Standards Roadmap Working Group [Internet]. Maryland: National Institute of Standards and Technology; [cited 2011 Aug 16]. Available from: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsRoadmap *"NIST is leading the development of a USG (US Government) Cloud Computing Technology Roadmap. This roadmap will define and prioritize USG requirements for interoperability, portability, and security for cloud computing in order to support secure and effective USG adoption of Cloud Computing."*

Table 2.2 SDOs and Other Community-Driven Organizations

Name	Acronym	Website
American National Standard Institute	ANSI	www.ansi.org
Distributed Management Task Force	DMTF	www.dmtf.org
International Telecommunication Union	ITU	www.itu.int
Institute of Electrical and Electronic Engineers	IEEE	standards.ieee.org www.ieee.org
International Organization for Standardization	ISO	www.iso.org
Electronic Industries Alliance/ Telecommunications Industry Association	EIA/TIA	www.eia.orgwww.tiaonline.org
Internet Engineering Task Force	IETF	www.ietf.org
Internet Assigned Numbers Authority	IANA	www.iana.org
National Institute of Standards and Technology (NIST)	NIST	www.nist.gov
Object Management Group	OMG	www.omg.org
Open Grid Forum	OGF	www.gridforum.org
OpenID Foundation	OpenID Foundation	openid.net
Organization for the Advancement of Structured Information Standards	OASIS	www.oasis-open.org
Storage Network Industry Association	SNIA	www.snia.org
TeleManagement Forum	TM Forum	www.tmforum.org
World Wide Web Consortium	W3C	www.w3.org
Web Services Interoperability Organization	WS-I	www.ws-i.org

applicable business and technical use cases. As previously discussed, this mapping activity is an important part in determining standards gaps and support prioritization with the standards community.

Table 2.3 Internet-Related Standards

Name	Organization	Document Reference (Publication Date)
Domain Name System (DNS)	IETF	RFC 1034 (11/1987)[a]RFC 1035 (11/1987)[b]
eXtensible Access Control Markup Language (XACML)	OASIS	XACML v2.0 (02/2005)[c]
Extensible Markup Language (XML)	W3C	XML v1.1 2nd Edition (08/2006)[d]
File Transfer Protocol (FTP)	IETF	RFC 959 (10/1985)[e]
Hypertext Transfer Protocol (HTTP)	IETF, W3C	HTTP v1.1, RFC 2616 (06/1999)[f]
HyperText Markup Language (HTML)	W3C	HTML v4.01 (12/2009)[g]HTML v5 (Draft) (05/2011)[h]
JavaScript Object Notation (JSON)	IETF (Douglas Crockford)	RFC 4627 (07/2006)[i]
Key Management Interoperability Protocol (KMIP)	OASIS KMIP TC	KMIP 1.0 (06/2010)[j]
OAuth (Open Authorization Protocol)	IETF, OAuth Working Group	1.0, RFC 5849 (04/2010),[k] 2.0 (09/2011)[l]
OpenID Authentication	OpenID Foundation	OpenID Authentication 2.0 (12/2007)[m]
REprentational State Transfer (REST)	University of California, Irvine (Roy Fielding)	Architectural Styles and the Design of Network-based Software Architectures (2000)[n]
Transmission Control Protocol/Internet Protocol (TCP/IP)	IETF	RFC 675 (12/1974)[o]RFC 791 (09/1981)[p]RFC 1180 (01/1991)[q]
Secure Sockets Layer (SSL)/Transport Layer Security (TLS)	Netscape Corporation (SSL Specification), IETF (TLS)	SSL v3.0 (1996)[r]TLS v1.2, RFC 5246 (08/2008)[s]
Security Assertion Markup Language (SAML)	OASIS Security Service TC	SAML 1.1 (09//2003),[t] 2.0 (03/2005)[u]
Service Provisioning Markup Language (SPML)	OASIS Provisioning Services TC	SPML v2.0 (04/2006)[v]
Simple Object Access Protocol (SOAP)	W3C, XML Protocol Working Group	SOAP v1.2 (06/2003)[w]
Simple Mail Transfer Protocol (SMTP)	IETF	SMTP RFC 5321 (10/2008)[x]
Web Services Addressing (WS-Addressing)	W3C	Web Services Addressing (WS-Addressing) (08/2004)[y] Web Services Addressing 1.0—SOAP Binding (05/2006)[z] Web Services Addressing 1.0—Metadata (09/2007)[aa]
Web Services Agreement Specification (WS-Agreement)	OGF	GFD.107: WS-Agreement 1.0 (03/2007)[ab]
Web Services Description Language (WSDL)	W3C	WSDL 1.1 (03/2001),[ac] v2.0 (06/2007)[ad]

Table 2.3 Internet-Related Standards (*continued*)

Name	Organization	Document Reference (Publication Date)
Web Services Federation (WSFED)	OASIS WSFED TC	WS-Federation 1.2 (03/2009)[ae]
Web Services Interoperability (WS-I) Basic Security Profile	WS-I	WS-I Basic Security Profile 1.0 (03/2007),[af] 1.1 (01/2010)[ag]
Web Services Interoperability (WS-I) Basic Profile	WS-I	WS-I Basic Profile 1.1 (08/2004),[ah] 1.2 (11/2010),[ai] 2.0 (11/2010)[aj]
Web Services Policy (WS-Policy)	W3C	Web Services Policy 1.5—Framework (09/2007)[ak] Web Services Policy 1.5—Attachment (09/2007)[al]
Web Services Reliable Exchange (WS-RX)	OASIS WS-RX TC	Web Services Reliable Messaging Policy Assertion (WS-RM Policy) (06/2007)[am] Web Services Reliable Messaging (WS-Reliable Messaging)1.2 (02/2009)[an] Web Services Make Connection (WS-MakeConnection) Version 1.1 (02/2009)[ao]
Web Services Resource Access (WS-RA)	W3C	Web Services Event Descriptions (WS-EventDescriptions) (Draft) (02/2010)[ap] WS-Eventing (03/2006)[aq] Web Services Fragment (WS-Fragment) (Draft) (03/2010)[ar] Web Services Metadata Exchange 1.1 (WS-MetadataExchange) (10/2008)[as] Web Services Transfer (WS-Transfer) (09/2006)[at]
Web Services Resource Framework (WSRF)	OASIS WSRF TC	WSRF 1.2 (04/2006)[au]
WS-Secure Conversation	OASIS WS-SX TC	WS-SecureConversation 1.3 (03/2007)[av]
Web Services Security (WSS)	OASIS WSS TC	Kerberos Token Profile 1.1 (02/2006)[aw] Rights Expression Language (REL) Token Profile 1.1 (02/2006)[ax] SAML Token Profile 1.1 (02/2006)[ay] SOAP with Attachments (SWA) Profile 1.1 (02/2006) [az] Username Token Profile 1.1 (02/2006)[ba] WS-Security Core Specification 1.1 (02/2006)[bb] X.509 Token Profile 1.1 (02/2006)[bc]

Table 2.3 Internet-Related Standards (*continued*)

Name	Organization	Document Reference (Publication Date)
Web Services Transaction (WS-TX)	OASIS WS-TX TC	Web Services Atomic Transaction (WS-AtomicTransaction) 1.2 (02/2009)[bd] Web Services Business Activity. (WS-BusinessActivity) (10/2008)[be] Web Services Coordination (WS-Coordination) 1.2 (02/2009)[bf]
Web Services Trust (WS-Trust)	OASIS WS-SX TC	WS-Trust 1.4 (02/2009)[bg]
XML Encryption Syntax and Processing	W3C	XML Encryption Syntax and Processing (12/2002)[bh]
XML Path Language (XPath) v1.0 and v2.0	W3C	XPath 1.0 (11/1999),[bi] 2.0 (01/2007)[bj]
X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	IETF	RFC 3820[bk]
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	IETF	RFC 3280 (06/2004)[bl]
XML Signature Syntax and Processing (XMLSig)	W3C	XMLSig 1.1 (03/2011),[bm] 2.0 (Draft) (04/2011)[bn]

[a] *Domain Names—Concepts and Facilities. Available from: http://www.ietf.org/rfc/rfc1034.txt.*

[b] *Domain Names—Implementation Specification. Available from: http://www.ietf.org/rfc/rfc1035.txt.*

[c] *Extensible Access Control Markup Language Version 2.0. Available from http://docs.oasis-open.org/xacml/2.0/XACML-2.0-OS-NORMATIVE.zip.*

[d] *Extensible Markup Language (XML) 1.1. Available from: http://www.w3.org/TR/xml11/.*

[e] *File Transfer Protocol. Available from: http://www.ietf.org/rfc/rfc959.txt.*

[f] *Hypertext Transfer Protocol 1.1. Available from http://www.ietf.org/rfc/rfc2616.txt.*

[g] *HyperText Markup Language 4.0.1. Available from: http://www.w3.org/TR/html401/.*

[h] *HyperText Markup Language 5. Available from: http://www.w3.org/TR/html5/.*

[i] *JavaScript Object Notation. Available from: http://www.ietf.org/rfc/rfc4627.txt.*

[j] *Key Management Interoperability Protocol Specification Version 1.0. Available from: http://docs.oasis-open.org/kmip/spec/v1.0/cs01/kmip-spec-1.0-cs-01.html.*

[k] *The OAuth 1.0 Protocol. Available from: http://tools.ietf.org/html/rfc5849.*

[l] *TheOAuth 2.0 Authorization Protocol. Available from: http://tools.ietf.org/html/draft-ietf-oauth-v2-21.*

[m] *OpenID Authentication 2.0. Available from: http://openid.net/specs/openid-authentication-2_0.html.*

[n] *Architectural Styles and the Design of Network-based Software Architectures. Available from: http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm.*

[o] *Specification of Internet Transmission Control Program. Available from: http://tools.ietf.org/html/rfc675.*

[p] *Internet Protocol. Available from: http://www.ietf.org/rfc/rfc791.txt.*

[q] *A TCP/IP Tutorial. Available from http://tools.ietf.org/html/rfc1180.*

Table 2.3 Internet-Related Standards (*continued*)

[r] *The SSL Protocol Version 3.0. Available from: http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt.*
[s] *The Transport Layer Security (TLS) Protocol Version 1.2. Available from: http://tools.ietf.org/html/rfc5246.*
[t] *Security Assertion Markup Language v1.1. Available from: http://www.oasis-open.org/standards#samlv1.1.*
[u] *Security Assertion Markup Language v2.0. Available from: http://www.oasis-open.org/standards#samlv2.0.*
[v] *Service Provisioning Markup Language Version 2. Available from: http://www.oasis-open.org/committees/download.php/17708/pstc-spml-2.0-os.zip.*
[w] *SOAP Version 1.2 Part 1: Messaging Framework. Available from: http://www.w3.org/TR/soap12-part1/.*
[x] *Simple Mail Transfer Protocol. Available from http://tools.ietf.org/html/rfc5321.*
[y] *Web Services Addressing. Available from: http://www.w3.org/Submission/ws-addressing/.*
[z] *Web Services Addressing 1.0—SOAP Binding. Available from: http://www.w3.org/TR/ws-addr-soap/.*
[aa] *Web Services Addressing 1.0—Metadata. Available from: http://www.w3.org/TR/ws-addr-metadata/.*
[ab] *Web Services Agreement Specification. Available from: http://www.ogf.org/documents/GFD.107.pdf.*
[ac] *Web Services Description Language 1.1. Available from: http://www.w3.org/TR/wsdl.*
[ad] *Web Services Description Language 2.0. Available from: http://www.w3.org/TR/wsdl20/.*
[ae] *Web Services Federation Language Version 1.2. Available from: http://www.oasis-open.org/committees/download.php/31658/ws-federation-1.2-spec-cs-01.doc.*
[af] *Basic Security Profile Version 1.0. Available from http://www.ws-i.org/profiles/basicsecurityprofile-1.0.html.*
[ag] *Basic Security Profile Version 1.1. Available from http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html.*
[ah] *Basic Profile Version 1.1. Available from: http://www.ws-i.org/profiles/basicprofile-1.1-2004-08-24.html.*
[ai] *Basic Profile Version 1.2. Available from: http://www.ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html.*
[aj] *Basic Profile Version 2.0. Available from: http://www.ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html.*
[ak] *Web Services Policy 1.5—Framework. Available from: http://www.w3.org/TR/ws-policy/.*
[al] *Web Services Policy 1.5—Attachment. Available from: http://www.w3.org/TR/ws-policy-attach/.*
[am] *Web Services Reliability Messaging Policy Assertion Version 1.2. Available from: http://docs.oasis-open.org/ws-rx/wsrmp/200702/wsrmp-1.2-spec-os.html.*
[an] *Web Services Reliability Messaging Version 1.2. Available from: http://docs.oasis-open.org/ws-rx/wsrm/200702/wsrm-1.2-spec-os.html.*
[ao] *Web Services Make Connection Version 1.1. Available from: http://docs.oasis-open.org/ws-rx/wsmc/200702/wsmc-1.1-spec-os.html.*
[ap] *Web Services Event Descriptions. Available from: http://www.w3.org/TR/2010/WD-ws-event-descriptions-20100209/.*
[aq] *Web Services Eventing. Available from: http://www.w3.org/Submission/WS-Eventing/.*
[ar] *Web Services Fragment. Available from: http://www.w3.org/TR/2010/WD-ws-fragment-20100330/.*
[as] *Web Services Metadata Exchange 1.1. Available from: http://www.w3.org/Submission/2008/SUBM-WS-MetadataExchange-20080813/.*
[at] *Web Services Transfer. Available from: http://www.w3.org/Submission/WS-Transfer/.*
[au] *Web Services Resource 1.2. Available from: http://docs.oasis-open.org/wsrf/wsrf-ws_resource-1.2-spec-os.pdf.*
[av] *WS-SecureConversation 1.3. Available from: http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.3/ws-secureconversation.html.*
[aw] *Web Services Security Kerberos Token Profile 1.1. Available from: http://www.oasis-open.org/committees/download.php/16788/wss-v1.1-spec-os-KerberosTokenProfile.pdf.*

Table 2.3 Internet-Related Standards (*continued*)

[ax] *Web Services Security Rights Expression Language Token Profile 1.1. Available from: http://www.oasis-open.org/committees/download.php/16687/oasis-wss-rel-token-profile-1.1.pdf.*
[ay] *Web Services Security: SAML Token Profile 1.1. Available from: http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf.*
[az] *Web Services Security SOAP Messages with Attachments Profile 1.1. Available from: http://www.oasis-open.org/committees/download.php/16672/wss-v1.1-spec-os-SwAProfile.pdf.*
[ba] *Web Services Security Username Token Profile 1.1. Available from: http://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf.*
[bb] *Web Services Security SOAP Message Security 1.1. Available from: http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf.*
[bc] *Web Services Security X.509 Certificate Token Profile 1.1. Available from: http://www.oasis-open.org/committees/download.php/16785/wss-v1.1-spec-os-x509TokenProfile.pdf.*
[bd] *Web Services Atomic Transaction Version 1.2. Available from: http://docs.oasis-open.org/ws-tx/wstx-wsat-1.2-spec.html.*
[be] *Web Services Business Activity Version 1.2. Available from: http://docs.oasis-open.org/ws-tx/wstx-wsba-1.2-spec-cs-01.pdf.*
[bf] *Web Services Coordination Version 1.2. Available from: http://docs.oasis-open.org/ws-tx/wstx-wscoor-1.2-spec.html*
[bg] *WS-Trust 1.4. Available from: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html.*
[bh] *XML Encryption Syntax and Processing. Available from: http://www.w3.org/TR/xmlenc-core/.*
[bi] *XML Path Language Version 1.0. Available from: http://www.w3.org/TR/xpath/.*
[bj] *XML Path Language Version 2.0. Available from: http://www.w3.org/TR/xpath20/.*
[bk] *Internet X.509 Public Key Infrastructure Proxy Certificate Profile. Available from: http://www.ietf.org/rfc/rfc3820.txt.*
[bl] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile. Available from: http://www.ietf.org/rfc/rfc3280.txt.*
[bm] *XML Signature Syntax and Processing Version 1.1. Available from: http://www.w3.org/TR/xmldsig-core1/.*
[bn] *XML Signature Syntax and Processing Version 2.0. Available from: http://www.w3.org/TR/xmldsig-core2/.*

Table 2.4 US Federal Government and International-Related Standards

Name	Organization	Document Reference (Publication Date)
Advanced Encryption Standard (AES)	NIST	Federal Information Processing Standard (FIPS) 197 (11/2001)[a]
Automated Password Generator (APG)	NIST	FIPS 181 (11/1993)[b]
Common vulnerabilities and exposures	NIST/MITRE, ITU-T Study Group 17, Question 4 (SG17/Q4)	National Vulnerability Database (NVD) 2.2[c] Recommendation X.1520 (04/2011)[d]
Common vulnerability scoring system	First.org, Inc., ITU-T Study Group 17, Question 4 (SG17/Q4)	CVSS 2.0 (06/2007)[e] NVD 2.2 Recommendation X.1521 (04/2011)[f]

Table 2.4 US Federal Government and Internet-Related Standards (*continued*)

Name	Organization	Document Reference (Publication Date)
Computer Security Incident Handling Guide	NIST	NIST Special Publication (SP) 800-61, Rev. 2 (08/2012)[g]
Digital Signature Standard (DSS)	NIST	FIPS 186-3 (06/2009)[h]
Entity Authentication Using Public Key Cryptography	NIST	FIPS 196 (02/1997)[i]
Escrowed Encryption Standard (EES)	NIST	FIPS 185 (02/1994)[j]
Guideline for Incident Preparedness and Operational continuity Management	ISO	ISO/PAS 22399:2007[k]
Guidelines for the Use of Advanced Authentication Technology Alternatives	NIST	FIPS 190 (09/1994)[l]
Minimum Security Requirements for Federal Information and Information Systems	NIST	FIPS 200 (03/2006)[m]
Overview of Cybersecurity information exchange (CYBEX)	ITU-T Study Group 17, Question 4 (SG17/Q4)	Recommendation X.1520 (04/2011)[n]
Personal Identity Verification (PIV) of Federal Employees and Contractors	NIST	FIPS 201-1, Change Notice 1 (03/2006)[o], 201-2 (Revised Draft) (07/2012)[p]
Security Content Automation Protocol (SCAP)	NIST	NIST Special Publication (SP) 800-126, 1.0 (11/2009)[q], 1.1 (02/2011)[r], 1.2 (09/2011)[s]
Secure Hash Standard (SHS)	NIST	FIPS, 180-4 (03/2012)[t]
Security Requirements for Cryptographic Modules	NIST	FIPS 140-2 (05/2001)[u], 140-3 (Draft) (12/2009)[v]
Standards for Security Categorization of Federal Information and Information System	NIST	FIPS 199 (02/2004)[w]
Standard Security Label for Information Transfer	NIST	FIPS 188 (09/1994)[x]
The Key-Hash Message Authentication Code (HMAC)	NIST	FIPS 198-1 (07/2008)[y]

Table 2.4 US Federal Government and Internet-Related Standards (*continued*)

[a] *Advanced Encryption Standard. Available from: http://csrc.nist.gov/publications/fips/fips197/fips197.pdf.*

[b] *Automated Password Generator. Available from: http://www.itl.nist.gov/fipspubs/fip181.htm.*

[c] *Natonal Vulnerability Database. Available from: http://nvd.nist.gov/.*

[d] *Cybersecurity information exchange—Vulnerability/state exchange: Common vulnerabilities and exposures. Available from: http://www.itu.int/rec/T-REC-X.1520-201104-I/en.*

[e] *A Complete Guide to the Common Vulnerability Scoring System Version 2.0. Available from: http://www.first.org/cvss/cvss-guide.html.*

[f] *Cybersecurity information exchange—Vulnerability/state exchange: Common vulnerability scoring system. Available from: http://www.itu.int/rec/T-REC-X.1521-201104-I.*

[g] *Computer Security Incident Handling Guide. Available from: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.*

[h] *Digital Signature Standard (DSS). Available from: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.*

[i] *Entity Authentication Using Public Key Cryptography. Available from: http://csrc.nist.gov/publications/fips/fips196/fips196.pdf.*

[j] *Escrowed Encryption Standards. Available from: http://www.itl.nist.gov/fipspubs/fip185.htm.*

[k] *Societal security—Guidelines for incident preparedness and operational continuity management. Available from: http://www.iso.org/iso/catalogue_detail?csnumber=50295.*

[l] *Guidelines for the Use of Advanced Authentication Technology Alternatives. Available from: http://csrc.nist.gov/publications/fips/fips190/fip190.txt.*

[m] *Minimum Security Requirements for Federal Information and Information Systems. Available from: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.*

[n] *Cybersecurity information exchange—Overview of cybersecurity: Overview of cybersecurity information exchange. Available from: http://www.itu.int/rec/T-REC-X.1500-201104-I/en.*

[o] *Personal Identity Verification (PIV) of Federal Employees and Contractors Version 1. Available from: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.*

[p] *Personal Identity Verification (PIV) of Federal Employees and Contractors (Draft) Version 2. Available from: http://csrc.nist.gov/publications/PubsDrafts.html#FIPS-201-2.*

[q] *The Technical Specification for the Security Content Automation Protocol (SCAP); SCAP Version 1.0. Available from: http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf.*

[r] *The Technical Specification for the Security Content Automation Protocol (SCAP); SCAP Version 1.1. Available from: http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf.*

[s] *The Technical Specification for the Security Content Automation Protocol (SCAP); SCAP Version 2.0. Available from: http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf.*

[t] *Secure Hash Standard (SHS) Available from: http://csrc.nist.gov/publications/PubsDrafts.html#FIPS-180-4.*

[u] *Security Requirements for Cryptographic Modules. Available from: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.*

[v] *Security Requirements for Cryptographic Modules (Draft). Available from: http://csrc.nist.gov/publications/PubsDrafts.html#FIPS-140–3.*

[w] *Standards for Security Categorization of Federal Information and Information Systems. Available from: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.*

[x] *Standards Security Label for Information Transfer. Available from: http://csrc.nist.gov/publications/fips/fips188/fips188.pdf.*

[y] *The Keyed-Hash Message Authentication code (HMAC). Available from: http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf.*

Table 2.5 Cloud Computing—Related Standards

Name	Organization	Document Reference (Publication Date)
Cloud Data Management Interface (CDMI)	SNIA	CDMI 1.0 (04/2010)[a], 1.0.1 (09/2011)[b], 1.0.2 (06/2012)[c]
Cloud Infrastructure Management Interface (CIMI)	DMTF	CIMI 1.0 (09/2012)[d]
Guide for Cloud Portability and Interoperability Profiles (CPIP)	IEEE, Cloud Profiles WG (CPWG) Working Group	IEEE P2301 (Draft)[e]
Job Submission Definition Language	OGF	GFD-R.56: JSDL v1.0 (07/2008)[f]
Open Cloud Computing Interface (OCCI)	OGF	GFD.P-R.183: OCCI–Core (06/2011)[g] GFD.P-R.184: OCCI-Infrastructure (06/2011)[h] GFD.P-R.185: RESTful HTTP Rendering (01/2011)[i]
Open Virtualization Format (OVF)	DMTF ISO/IEC	OVF v1.1.0 (01/2010)[j] ISO/IEC 17203: 2011[k]
Requirement of IdM in cloud computing	ITU-T Study Group 17, Question 4 (SG17/Q4)	XX.idmcc (Draft) (4/2011)[l]
Standard for Intercloud Interoperability and Federation (SIIF)	IEEE, Intercloud WG (ICWG) Working Group	IEEE P2302 (Draft)[m]
Usage Record (UR)	OGF	GFD-R. .098: Usage Record (9/2006). 98.[n]

[a] *Cloud Data Management Interface Version 1.0. Available from: http://snia.org/sites/default/files/CDMI_SNIA_Architecture_v1.0.pdf.*

[b] *Cloud Data Management Interface Version 1.0.1. Available from: http://snia.org/sites/default/files/CDMI_SNIA_Architecture_v1.0.1.pdf.*

[c] *Cloud Data Management Interface Version 1.0.2. Available from: http://snia.org/sites/default/files/CDMI/20v1.0.2.pdf.*

[d] *Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol. Available from: http://dmtf.org/sites/default/files/standards/documents/DSP0263_1.0.0.pdf.*

[e] *Guide for Cloud Portability and Interoperability Profiles. Available from: http://standards.ieee.org/develop/project/2301.html.*

[f] *Job Submissions Definition Language. Available from: http://www.gridforum.org/documents/GFD.56.pdf.*

[g] *Open Cloud Computing Interface—Core. Available from: http://www.ogf.org/documents/GFD.183.pdf.*

[h] *Open Cloud Computing Interface—Infrastructure. Available from: http://www.ogf.org/documents/GFD.184.pdf.*

[i] *Open Cloud Computing Interface—RESTful HTTP Rendering. Available from: http://www.gridforum.org/documents/GFD.185.pdf.*

[j] *Open Virtualization Format Specification. Available from: http://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf.*

[k] *Information technology—Open Virtualization Format (OVF) specification. Available from: http://www.iso.org/iso/iso_catalogue_detail.htm? csnumber=59388.*

[l] *Requirements of IdM in cloud computing. Available from: http://www.itu.int/md/T09-SG17-110411-TD-PLEN-1675.*

[m] *Standard for Intercloud Interoperability and Federation. Available from: http://standards.ieee.org/develop/project/2302.html.*

[n] *Usage Record—Format Recommendation. Available from: http://www.gridforum.org/documents/GFD.98.pdf.*

SUMMARY

This chapter provided an overview of the standards activities and the importance of standards development to the adoption of cloud computing within the federal government. By briefly reviewing the standards development process, we can begin to characterize standards supporting cloud computing and their maturity based on the evolutionary standards life cycle. We then discussed the federal legislative and policy drivers that address the federal government's role in supporting standards activities and the drivers affecting cloud computing adoption. We concluded our discussion by looking at the NIST Conceptual Reference Model and how the reference architecture can be used to facilitate the identification of standards that would meet specific usage scenarios.

References

[1] National Institute of Standards and Technology (NIST). NIST Cloud Computing Standards Roadmap Working Group, Hogan H, Liu F, Sokol A, Tong J. NIST Special Publication (SP) 500-291, NIST cloud computing standards roadmap. Maryland: National Institute of Standards and Technology; 2011.

[2] National Institute of Standards and Technology (NIST). National Technology Transfer and Advancement Act (NTTAA) [Internet]. Maryland: National Institute of Standards and Technology [cited August 15, 2011]. <http://standards.gov/nttaa.cfm>.

[3] Kundra V. Federal cloud computing strategy. Washington: Executive Office of the President, Office of Management and Budget; 2011.

[4] Mell P, Grance T. NIST Special Publication (SP) 800-145, The NIST definition of cloud computing. Maryland: National Institute of Standards and Technology; 2011.

[5] United States Standards Strategy Committee United States Standards Strategy. New York: American National Standards Institute; 2010.

[6] National Institute of Standards and Technology (NIST). NIST Standards acceleration to jumpstart adoption of cloud computing (SAJACC) [Internet]. Maryland: National Institute of Standards and Technology [cited August 22, 2011]. <http://www.nist.gov/itl/cloud/sajacc.cfm>.

[7] DeVaux C. NIST Interagency Report (IR) IR 6802, A guide to documenting standards. Maryland: National Institute of Standards and Technology; 2001.

[8] US House of Representatives Trade Agreements Act of 1979 [Internet]. Washington: US House of Representatives [cited August 23, 2011]. <http://uscode.house.gov/download/pls/19C13.txt>.

[9] National Institute of Standards and Technology (NIST). NIST National Technology Transfer and Advancement Act (NTTAA) [Internet]. Maryland: National Institute of Standards and Technology [cited August 24, 2011]. <http://standards.gov/nttaa.cfm>.

[10] Office of Management and Budget (OMB) Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities [Internet]. Washington: Executive Office of the President, Office of Management and Budget [cited August 25, 2011]. <http://www.whitehouse.gov/omb/circulars_a119>.

[11] America Competes Reauthorization Act of 2010 [Internet]. Washington: US Government Printing Office [cited August 23, 2011]. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ358/html/PLAW-111publ358.htm>.

[12] Mell P, Grance T. NIST Special Publication (SP) 800-145, The NIST definition of cloud computing. Maryland: National Institute of Standards and Technology; 2011.

[13] Fang L, Tong J, Mao J, Bohn R, Messina J, Badger L et al. NIST Special Publication (SP) 500-292, NIST cloud computing standards roadmap. Maryland: National Institute of Standards and Technology; 2011.

[14] Federal CIO Council and Chief Acquisition Officers Council. Creating effective cloud computing contracts for the federal government. Washington: Executive Office of the President, Office of Management and Budget; 2012.

CHAPTER

A Case for Open Source

3

INFORMATION IN THIS CHAPTER:

- Introduction
- Open Source and the Federal Government
- OSS Adoption Challenges: Acquisition and Security
- OSS and Federal Cloud Computing

INTRODUCTION

There has been a continued growth in the use of open source software or OSS[1] and cloud computing, both in the public and private sector. In this chapter, we will focus our discussion on the impact of OSS and the federal government's adoption of cloud computing technologies. Both cloud computing and OSS[2] individually offer potential benefits for federal agencies to improve their efficiency, agility, and innovation, by enabling them to be more responsive to new or changing requirements in their missions. OSS improves the way the federal government develops and also distributes software and provides an opportunity to reduce costs through the reuse of existing source code, whereas cloud computing improves the utilization of resources and enables a faster service delivery. This chapter does not attempt to differentiate OSS from proprietary software, but instead focuses on highlighting the importance in the federal government's experience with OSS in the adoption of cloud computing.[3]

[1] From Wennergren, D. Clarifying Guidance Regarding Open Source Software (OSS). Washington: US Department of Defense; 2009. *"Open software is software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software."*

[2] Some examples include operating systems (*Linux, Solaris*), web/middlewares (*Apache, JBoss Glassfish*), databases (*MySQLP, PostgreSQL*), applications (*Firefox, Thunderbird*), and programming languages (*Perl, Python, PHP*).

[3] *NASA Nebula Cloud Computing Platform*. Available from: http://nebula.nasa.gov/.

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00003-4

Over the years, the private sector[4] had encouraged the federal government to consider OSS by making a case for open source options. Many federal agencies have approached OSS with cautious interest because of challenges and concerns associated with its adoption. For example, transition costs, limited or in consistent skillset for open source software developers within the federal workforce, a lack of knowledge regarding procurement or licensing, and the misinterpretation of acquisition and security policies and guidance are some of the challenges and concerns that have limited a broader-scale adoption. However, some federal agencies have directly or indirectly made considerations for OSS as a viable enterprise-wide alternative to proprietary commercial off the shelf (COTS) software.

NOTE

Example cases where OSS was identified as a viable option to support federal government programs:

- In May 2011, the US Department of Veterans Affair (VA) CIO stated to avoid costs, and to find a way to involve the private sector in modernizing Veterans Integrated System Technology Architecture (VistA; *electronic medical records system*), the VA turned to open source [1]. In response, the VA launched the Open Source Electronic Health Record Agent (OSEHRA) in August 2012 "as a central governing body of a new open source Electronic Health Record (EHR) community" [2].
- In January 2012, the National Aeronautics and Space Administration (NASA) launched a new website, the NASA Open Government Initiative,[5] to expand the agency's open source software development. The NASA Open Government co-lead stated "We believe tomorrow's space and science systems will be built in the open, and that code.nasa.gov will play a big part in getting us there" [3].

Interoperability, portability, and security standards[6] have already been identified[7] as critical barriers for cloud adoption by the federal government. OSS facilitates supporting standards development through the "shared" development and industry implementation of open standards.[8] In some instances, the federal government's experience with standards development had enabled the broader adoption and use of open standards–based, open source technologies and platforms.[9] The primarily driver

[4] For example, the Open Source for America (OSfA) is an effort to raise awareness in the federal government about the benefits of open source software. Available from: http://opensourceforamerica.org/.
[5] *NASA Open Government Initiative*. Available from: http://www.nasa.gov/open/.
[6] Standards were discussed in detail in Chapter 2, Cloud Computing Standards.
[7] From Kundra, V. *Federal Cloud Computing Strategy*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. *Standards will be critical for the successful adoption and delivery of cloud computing, both within the public sector and more broadly. Standards are also critical to ensure clouds have an interoperable platform so that services provided by different providers can work together, regardless of whether they are provided using public, private, community, or a hybrid delivery model.*
[8] Open standards, in general terms, is a technical specification which is developed openly (participation and publication) and is vendor neutral with limited cost (or free availability) to implementers.
[9] Examples include GSA's Apps.gov. Available from: https://www.apps.gov/cloud/cloud/category_home.do?&c=SA.

is to enable solutions to be developed through the integration of multiple frameworks and products while at the same time easing concerns over interoperability and portability. For example, in Chapter 2, interoperability, portability, and security standards were identified as critical barriers for the broader cloud adoption, both in the federal government and the private sector. OSS facilitates overcoming these standards obstacles through the development and implementation of open standards.

In addition, OSS also enables agility within the software development by supporting an agile procurement process where the federal agencies can more rapidly acquire/deploy technologies and capabilities. For example, many modernization projects have identified the use of open source software as a more economical value for the federal government. Through the use of smaller, agile procurements, federal agencies can achieve a higher yield and greater return on investment (ROI) compared to slower, inefficient long-term investments that use traditional procurement methods that tend to be outpaced by private sector innovations due to lengthy development cycles. Additionally, federal agencies are required to consider multiple factors when defining the overall business case[10] for an IT investment.[11] Some such factors that must be considered as part of the IT investment decision-making process[12] includes the total cost of ownership and lifecycle maintenance costs, the costs associated with mitigating security risks, and the security and privacy of data [4]. OSS also requires transitioning to a subscription-based model, there by reducing the burden for federal agencies to invest in upfront costs which lock them into capital expenses that may be unrecoverable if the requirements change or a program is canceled or rescoped.

OPEN SOURCE AND THE FEDERAL GOVERNMENT

The US government's use of OSS has its beginning in the 1990s.[13] During this period, OSS was used primarily within the research and scientific community where collaboration and information sharing[14] was a cultural norm. However, it was not until 2000 that the federal government began to seriously consider the use of OSS as a model for accelerating innovation within the federal government. As illustrated in Figure 3.1, the federal government has developed a list of OSS-related studies, policies, and guidelines that have formed the basis for the policy framework that has

[10] Guidance on exhibit 300A (business cases). Available from: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy13_guidance_for_exhibit_300_a-b_20110715.pdf.

[11] From Office of Management and Budget (OMB). OMB Circular A-11, Planning, Budgeting, and Acquisition of Capital Assets. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. *"Agencies should make security's role explicit in information technology investments and capital programming"*.

[12] The Capital Planning and Investment Control Process (CPIC) includes a requirement to integrate IT security into the IT investment evaluation criteria. Available from: http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf.

[13] *Timeline: A History of Open Source in Government.* Available from: http://gov-oss.org/.

[14] *Intranet Hallways Systems Based on Linux.* Available from: http://linuxgazette.net/issue19/hallways.html.

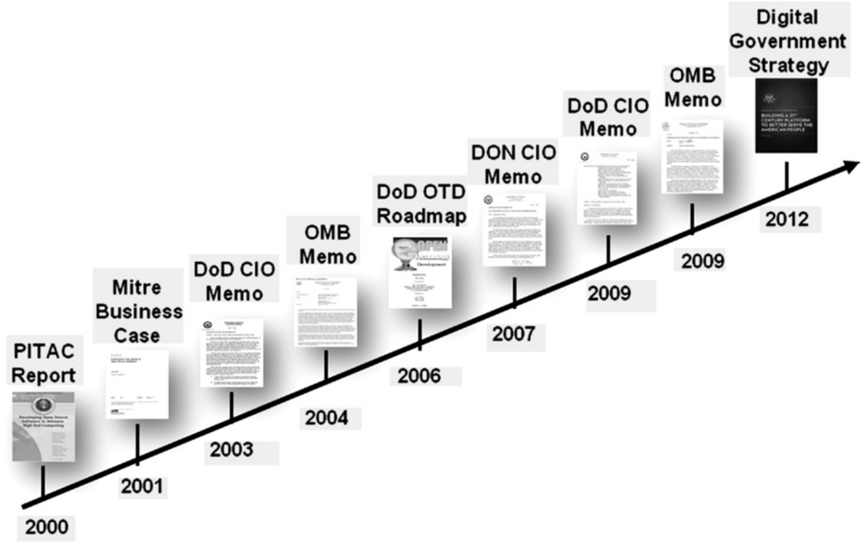


FIGURE 3.1 US Government OSS Policy Framework

guided the adoption of OSS. This framework tackles critical issues that have inhibited the federal government from attaining the full benefits offered by OSS. Although gaps[15] still exist in specific guidelines relating to the evaluation, contribution, and sharing of OSS, the policy framework serves as a foundation for guiding federal agencies in the use of OSS by reducing barriers that have limited a broader adoption. In this section we will explore the policy framework with the objective of describing how the current policy framework has led to the broader use of OSS across the federal government, and more importantly how this framework has enabled the federal government's adoption of cloud computing by overcoming the challenges with acquisition and security that will be discussed in detail in the next section.

The President's Information Technology Advisory Committee (PITAC),[16] which examined OSS, was given the goal [5] of:

- Charting a vision of how the federal government can support developing open source software;
- Defining a policy framework;
- Identifying policy, legal, and administrative barriers to the widespread adoption of OSS; and
- Identifying potential roles for public institutions in OSS economics model.

[15] Lessons Learned: Roadblocks and Opportunities for Open Source Software (OSS) in US Government.

[16] Co-Chaired by Raj Reddy of Carnegie Mellon University (http://www.rr.cs.cmu.edu/) and Irving Wladawsky-Berger of MIT (http://esd.mit.edu/people/scholars/wladawsky-berger/wladaws'ky-berger.htm).

Table 3.1 Advantages and Challenges Highlighted in the PITAC Report [5]

Advantages	• Potentially improved security because programmers have developed access to source code that allows them to examine it for potential embedded trap doors and/or Trojan horses
	• Increase in the number of programmers searching for software bugs and developing fixes
Challenges	• Limitation in the project management and funding models to support "fiscal flexibility" for open source development
	• Lack of policies or guidance governing export control and national security considerations
	• Potentially incompatible licensing agreements used within the open source community may cause delays due to the lack of education of how to use them
	• Poorly defined procurement rules do not explicitly authorize competition between open source alternatives and proprietary software
	• Lack of clear guidance regarding the decision-making authority and/or responsibility of the federal agency to use open source software
	• Lack of a single repository for warehousing open source projects

The PITAC published a report[17] concluded that the use of the open source development model (also known as the Bazaar model[18]) was a viable strategy for producing high quality software through a mixture of public, private, and academic partnerships [6]. In addition, as presented in Table 3.1, the report also highlighted several advantages and challenges. Some of these key issues have been at the forefront of the federal government's adoption of OSS.

Over the years since the PITAC report, the federal government has gained significant experience in both sponsoring and contributing to OSS projects. For example, one of the most-widely recognized contributions by the federal government specifically related to security is the Security Enhanced Linux (SELinux) project.[19] The SELinux project focused on improving the Linux kernel through the development of a reference implementation of the Flask security architecture[20] for flexible mandatory access control (MAC). In 2000, the National Security Agency (NSA)[21] made the

[17] *Developing Open Source Software to Advance High End Computing*. Available from: http://www.nitrd.gov/pitac/report/index.html.

[18] *The Cathedral and the Bazaar*. Available from: http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/index.html.

[19] *SELinux Frequently Asked Questions (FAQ)*. Available from: http://www.nsa.gov/research/selinux/faqs.shtml#I1.

[20] *Flask security architecture*. Available from: http://www.cs.utah.edu/flux/fluke/html/flask.html.

[21] *NSA SELinux Press Release*. Available from: http://www.nsa.gov/public_info/press_room/2001/se-linux.shtml.

SELinux available to the Linux community under the terms of the GNU's Not Unix (GNU) General Public License (GPL).[22]

NOTE

The Open Source Definition (OSD)[23] had its beginning as free software[24] in the early 1980s during the free software movement[25] starting with the GNU[26] project[27] which implemented the GPL. Although the early uses of the term "open source" and "free software" had been used interchangeably during that period, it was not until 1998 that Netscape Communications Corporation released[28] their Netscape Navigator Web browser source code as Mozilla. At this time, the distinction of the "open source"[29] concept became more mainstream within the broader commercial software industry. The *Free Software Foundation*[30] and *Open Source Initiative (OSI)*[31] have similar goals, but there was a notable difference in respect to their philosophies[32] and approved licenses.[33]

Starting in 2001, the MITRE Corporation, for the US Department of Defense (DoD), published a report[34] that built a business case for the DoD's use of OSS. The business case discussed both the benefits and risks for considering OSS. In MITRE's conclusion, OSS offered significant benefits to the federal government, such as improved interoperability, increased support for open standards and quality, lower costs, and agility through reduced development time. In addition, MITRE highlighted issues and risks, recommending any consideration of OSS should be carefully reviewed.

Shortly after the MITRE report, the federal government began to establish specific policies and guidance to help clarify issues around OSS. The DoD Chief

[22] *GNU General Public License*. Available from: http://www.gnu.org/copyleft/gpl.html.

[23] Based loosely on the *Debian Software Guidelines (DFSG)*. Available from: http://www.debian.org/social_contract#guidelines.

[24] *The Free Software Definition*. Available from: http://www.gnu.org/philosophy/free-sw.html.

[25] *Why Software Should Not Have Owners*. Available from: http://www.gnu.org/philosophy/why-free.html.

[26] *GNU Not For Unix*. Available from: http://www.gnu.org/gnu/manifesto.html.

[27] The Free Software Foundation was a sponsoring organization of GNU.

[28] *The Beginning of Mozilla*. Available from: http://blog.lizardwrangler.com/2008/01/22/january-22-1998-the-beginning-of-mozilla/.

[29] *The Cathedral and the Bazaar*. Available from: http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/.

[30] *Free Software Foundation (FSF)*. Available from: http://www.fsf.org/.

[31] *Open Source Initiative (OSI)*. Available from: http://www.opensource.org/.

[32] *Why Open Source missed the point of Free Software*. Available from: http://www.gnu.org/philosophy/open-source-misses-the-point.html.

[33] *OSI Approved Licenses*. Available from: http://www.opensource.org/licenses/alphabetical and *Free Software Foundation Licenses*. Available from: http://en.wikipedia.org/wiki/List_of_FSF_approved_software_licenses.

[34] *Making a Business Case for Open Source*. Available from: http://www.mitre.org/work/tech_papers/tech_papers_01/kenwood_software/kenwood_software.pdf.

Information Officer (CIO) published the department's first official DoD-wide memorandum to reiterate existing policy and to provide clarifying guidance on the acquisition, development, and the use of OSS within the DoD community [7]. Soon after the DoD policy, the Office of Management and Budget (OMB) established a memorandum to provide government-wide policy[35] regarding acquisition[36] and licensing issues.

Since 2003, there were multiple misconceptions, specifically within the DoD regarding the use of OSS. Therefore, in 2007, the US Department of the Navy (DON) CIO released a memorandum[37] which clarified the classification of OSS and directed the Department to identify areas where OSS can be used within the DONs Information Technology (IT) portfolio. This was followed by another DoD-wide memorandum in 2009, which provided DoD-wide guidance and clarified the use and development of OSS, including explaining the potential advantages of the DoD reducing the development time for new software, anticipating threats, and response to continual changes in requirements [8].

In 2009, OMB released the *Open Government Directive*[38] which required federal agencies to develop and publish an Open Government Plan on their websites. The Open Government Plan[39] provided a description on how federal agencies would improve transparency and integrate public participation and collaboration [9]. As an example response to the directive support for openness, the National Aeronautics and Space Administration (NASA) in furtherance of its Open Government Plan released the "open.NASA"[40] site which was built completely using OSS, such as the LAMP stack[41] and Wordpress content management system (CMS).

[35] Office of Management and Budget (OMB) Memorandum 04-16, *Software Acquisition.* Available from: http://www.whitehouse.gov/omb/memoranda_fy04_m04-16.

[36] From Evans, K., Burton, R. Office of Management and Budget (OMB) Memorandum 04-16, Software Acquisition. Washington, DC: Executive Office of the President, Office of Management and Budget; 2004. *The Office of Management and Budget (OMB) Circulars A-11 and A-130 and the Federal Acquisition Regulation (FAR), guide agency information technology (IT) investment decisions and are intentionally technology and vendor neutral.*

[37] *Department of the Navy Open Source Software Guidance.* Available from: http://www.doncio.navy.mil/ContentView.aspx?ID=312.

[38] From Transparency and Open Government [Internet]. Washington, DC: The White House [cited 2012 June 2]. Available from: http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government. *In 2009, a Presidential Memoranda was issued titled "Transparency and Open Government" which directed the OMB Director to issue an Open Government Directive to instruct federal agencies to take specific action in implementing the Open Government Initiative.*

[39] NASA released its original Open Government Plan 1.0 in April of 2010 and in accordance with the requirement to review/update every two years under the *Open Government Directive,* NASA's current Open Government Plan was released in April of 2012. Available from: http://www.nasa.gov/open/plan/.

[40] *open.NASA*. Available from: http://open.nasa.gov.

[41] Linux, Apache, MySQL, and Perl/PHP (LAMP).

More recently, the White House's release of the *Digital Government Strategy* complemented[42] other initiatives and established principles for transforming the federal government. More specifically, the strategy outlined the need for a "shared platform" approach. In this approach, the federal government would need to leverage "sharing" of resources such as the "use of open source technologies that enable more sharing of data and make content more accessible" [10].

In this section we discussed key milestones that have impacted the federal government's cultural acceptance of OSS. It also discussed the current policy framework that has been developed through a series of policies and guidelines to support federal agencies in the adoption of OSS and the establishment of processes and policies to encourage and support the development of OSS. The remainder of this chapter will examine the key issues that have impacted OSS adoption and briefly examine the role of OSS in the adoption of cloud computing within the federal government.

OSS ADOPTION CHALLENGES: ACQUISITION AND SECURITY

The adoption of OSS as previously mentioned, has faced a number of roadblocks within the federal government. In this section, we will focus our examination specifically on the *acquisition* and *security* challenges that have been key inhibitors in the broad adoption of OSS. In addition, through our review we will obtain a better understanding of how the federal government's relationship with OSS has changed over time and gain some insight into how this experience has eased the path to cloud computing.

NOTE

In a blog post titled "Streaming at 1:00: In the Cloud" [11], former US CIO Vivek Kundra noted three critical challenges facing the federal government in deploying new IT services and products:

- Procurement processes can be confusing and time-consuming.
- Security procedures are complex, costly, lengthy, and duplicative across agencies.
- Our (federal government) policies lag behind new trends, causing unnecessary restrictions on the use of new technology.

[42] From The White House. Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. *"The Digital Government Strategy complements several initiatives aimed at building a 21st century government that works better for the American people. These include Executive Order 13571 (Streamlining Service Delivery and Improving Customer Service), Executive Order 13576 (Delivering an Efficient, Effective, and Accountable Government), the President's Memorandum on Transparency and Open Government, OMB Memorandum M-10-06 (Open Government Directive), the National Strategy for Trusted Identities in Cyberspace (NSTIC), and the 25-Point Implementation Plan to Reform Federal Information Technology Management (IT Reform)."*

Acquisition Challenges

In the past, federal agencies have relied upon limited acquisition policy guidance[43] when considering the procurement and the use of OSS. In the PITAC report [12] discussed previously, two specific acquisition-related findings were highlighted:

- *Licensing agreements*—numerous licensing agreements, incompatible licensing requirements, and educating federal managers on open source licenses and conditions.[44]
- *Federal procurement rules*—no explicit authorization of competition between open source alternatives and proprietary software, and lack of guidance on applicability and usage of open source software.

Even with the limited policies guidance, federal agencies were required to understand how federal laws and regulations applied to the acquisition of OSS. Table 3.2 provides several references within federal laws and regulations that must be considered by federal agencies when procuring OSS (and other proprietary) COTS products.

In addition, federal agencies are also required to understand how to select and apply the various types of software licenses, specifically "where future modifications by the US government may be necessary" [13]. Guidelines in developing license criteria [14] used in determining which OSS license to use could include:

- Using an existing OSS license; not creating a new OSS license.
- Making sure it is actually OSS.
- Using a GPL-compatible license.
- Choosing a license that meets the expected uses of the OSS.
- Using a common OSS license.

In order to dispel concerns over these license issues, several policy documents were issued to govern acquisition and provide guidance on the use of OSS within the federal government. The OSS acquisition policy framework, outlined in Table 3.3, consists primarily of the existing OMB and DoD policies; however, some federal agencies have issued additional guidance[45] to provide specific guidance on how OSS could be used to support their specific mission and business requirements.

[43] Federal Acquisition Regulation (FAR). Washington: US General Services Administration; 2011. *"The Federal Acquisition Regulation (FAR) classifies open source software as commercial computer software" (or "commercial item means")—(1) customarily used by the general public or by non-governmental entities and (1)(i) sold, leased, or licensed to the general public; or (1)(ii) offered for sale, lease, or license to the general public.*

[44] MITRE study conducted in 2003, *"Use of Free and Open Source Software (FOSS) in the US Department of Defense."* Available from: http://dodcio.defense.gov/Portals/0/Documents/FOSS/dodfoss_pdf.pdf.

[45] For example, Internal Revenue Service (http://www.irs.gov/pub/irs-utl/fti-in-opensourcesoftware.doc), the Consumer Financial Protection Bureau (http://www.consumerfinance.gov/developers/sourcecode-policy/), and NASA (http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=2210&s=1C).

Table 3.2 Federal Laws and Regulations

Federal Laws	• 41 U.S.C. § 430[a]—Definitions (defines "commercial item")
	• 41 U.S.C. § 431[b]—Commercially available off-the-shelf item acquisitions: lists of inapplicable laws in Federal Acquisition Regulation (defines "Commercially available off-the-shelf (COTS) item")
	• 41 U.S.C. § 264B[c] and 10 USC § 2377[d]—Preference for acquisition of commercial items
Regulations	• Federal Acquisition Regulation (FAR) 2.101(b)[e], 12.000, 12.101(c)[f]—Acquisition of Commercial Items
	• FAR 10.001[g]—Market Research

[a] *Available from: http://www.gpo.gov/fdsys/pkg/USCODE-2009-title41/html/USCODE-2009-title41-chap7-sec403.htm.*
[b] *Available from: http://www.gpo.gov/fdsys/pkg/USCODE-2009-title41/html/USCODE-2009-title41-chap7-sec431.htm.*
[c] *Available from: http://www.gpo.gov/fdsys/pkg/USCODE-2009-title41/html/USCODE-2009-title41-chap4-subchapIV-sec264b.htm.*
[d] *Available from: http://www.gpo.gov/fdsys/pkg/USCODE-2006-title10/html/USCODE-2006-title10-subtitleA-partIV-chap140-sec2377.htm.*
[e] *Available from: https://www.acquisition.gov/far/html/Subpart%202_1.html.*
[f] *Available from: https://www.acquisition.gov/far/html/Subpart%2012_1.html.*
[g] *Available from: https://www.acquisition.gov/far/html/Subpart%202_1.html.*

In addition to the policy documents, several frequently asked questions (FAQs) have been developed to facilitate understanding key acquisition-related issues (see Table 3.4).

Security Challenges

OSS has previously been characterized as offering a number of potential security advantages. The security advantages include the ability for developers to access the source code, allowing for a more thorough examination and identification of security vulnerabilities, and an increased number of availability of programmers searching for bugs and subsequently developing fixes [12]. However, some of the same advantages have also been overshadowed by hindrances such as uncertainty of the trustworthiness of code repositories and the availability of source code to allow malicious attackers the ability to identify security vulnerabilities.

Challenges associated with security in OSS have also existed because there has been a lack of clarification and education of the processes and certifications required to ensure software is validated for use within the federal government. Some of the commonly used processes[46] and certification methodologies that are required for

[46] Certification and accreditation processes are discussed in detail in Chapter 7, Comparison of Federal and International Security Certification Standards.

Table 3.3 OSS Acquisition Policy Framework

OMB Memorandum 04-16, Software Acquisition (2004)[a]	• Clarified the equal treatment of OSS and proprietary software in acquisition decision • Recommended caution when using OSS to understand the type of OSS license associated with software and obligations to make original source available • Employee education of licensing restrictions
Clarifying Guidance Regarding Open Source Software (2009)[b]	• Clarified the applicability of OSS in meeting the definition of "commercial software" in accordance with 10 U.S.C 2377 • Requirement for conducting market research when preparing for procurement of property or services, including OSS • Clarified DoD Intruction 8500.2,[c] Information Assurance (IA) Implementation—DCPD-1 Public Domain Software Controls, does not forbid usage of OSS • All software, including OSS, should include maintenance and support • Clarified misconceptions of requirements to distribute modified OSS to public and emphasized importance of understanding which licenses allow users to modify *for internal use only* • Required the usage of a DoD-wide collaborative software development environment to distribute software source code and design documents • Distribution of OSS, including code fixes and enhancement, to the public when it is determined it is in the government's interest; the government has rights to reproduce and release, and public release of item is not restricted by other law or regulations (e.g., Export Administration Regulations (EAR)[d] or International Traffic in Arms Regulation[e] (ITAR))

[a] *From Evans, K., Burton, A. Office of Management and Budget (OMB) Memorandum 04-16, Software Acquisition. Washington, DC: Executive Office of the President, Office of Management and Budget; 2004. "The Office of Management and Budget (OMB) Circulars A-11 and A-130 and the Federal Acquisition Regulation (FAR), guide agency information technology (IT) investment decisions."*

[b] *DoD Instruction 8510.01. Available from: http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf.*

[c] *From Stenbit, J. DoD Instruction 8500.2 Information Assurance (IA) Implementation. Washington: US Department of Defense; 2003. The DoD memo also dispelled the misconceptions that OSS is classified as "freeware or shareware" which is prohibited from being "used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available."*

[d] *DoD Instruction 8510.01. Available from: http://www.bis.doc.gov/policiesandregulations/index.htm.*

[e] *International Traffic in Arms Regulation (ITAR). Available from: http://pmddtc.state.gov/regulations_laws/itar.html.*

Table 3.4 US Government OSS FAQs

Frequently asked questions regarding open source software (OSS) and the U.S. Department of Defense (DoD)(2009)	"An educational resource for government employees and government contractors to understand the policies and legal issues relating to the use of open source software (OSS) in the DoD" [15]
Frequently asked questions about copyright and computer software: issues affecting the US Government with Special Emphasis on Open Source Software (2010)	"Provides general guidance on a special category of copyright works—computer software—and includes a details discussion of open source software" [16]

verifying that software and applications meet federal security requirements include, but are not limited to:

- NIST Risk Management Framework (RMF).[47]
- DoD Information Assurance Security Certification and Accreditation Process (DIACAP).[48]
- National Information Assurance Certification and Accreditation Process (NIACAP).[49]
- National Information Assurance Partnership (NIAP), Common Criteria (CC).[50]

In addressing the challenges with OSS security, the federal government initiated a number of programs "to investigate open security methods, models and technologies and identify viable and sustainable approaches that support national cyber security objectives" [17]. For example, the US Department of Homeland Security (DHS), Science and Technology (S&T) Directorate Cyber Security Research and Development Center (CSRDC) manages the Homeland Open Security Technology (HOST)[51] program which is an information portal for open-source security tools and application. In addition, the DHS also initiated the Open Source Hardening Project to maintain a database of analyzed OSS using the Coverity scan.[52] The Scan website offers qualified project developers of open source software with a portal where they can retrieve defects identified by Prevent[53] analyses [18].

[47] NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. Available from: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[48] DoD Instruction 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*. Available from: www.dtic.mil/whs/directives/corres/pdf/851001p.pdf.

[49] NSTISSI-1000, *National Information Assurance Certification and Accreditation Process (NIACAP)*. Available from: http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf.

[50] *National Informational Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS)*. http://www.niap-ccevs.org/.

[51] *Homeland Open Security Technology (HOST)*. Available from: http://www.cyber.st.dhs.gov/host/.

[52] List of open source software scanned by the Coverity® Scan. Available from: http://www.scan.coverity.com/all-projects.html.

[53] Coverity provides the results of its static-analysis code inspection tool for free to open source community.

OSS AND FEDERAL CLOUD COMPUTING

Open source technologies have played a significant role in the federal government's adoption of cloud computing. From the inception of the *25-Point Implementation Plan to Reform Federal Information Technology Management,* which introduced the key components of the federal government's adoption of "light technologies" and "shared solutions," the federal government has initiated the shift toward more openness and shared platforms. Openness and shared platforms support the ability of the federal government to deliver agility and innovation. OSS has served as the enabler, spawning incubations[54] in technologies across the industry and public sector that have formed the foundation of many of the cloud computing platforms.

The Federal Data Center Consolidation Initiative (FDCCI) is a federal consolidation effort focused on reducing physical space by shifting IT investments to more efficient computing platforms and technologies [21]. These computing platforms and

NOTE

In 2003, NASA began "assessing the formal barriers to distributing software they developed as open source and began reviewing the state of open source licenses"[55] [19]. Open source[56] directly addressed NASA's needs of the rapid and wide dissemination of software with minimal overhead and cost, supporting its functions under the National Aeronautics and Space Act.[57] However, it was not until September 15, 2009, when the former US CIO Vivek Kundra announced the launch of Apps.gov[58] at the NASA Ames Research Center (ARC),[59] did it set the stage for the next phase in the federal government's adoption of public cloud computing services. During this time, NASA ARC had already begun an effort in the development of a cloud environment through the Nebula project.[60] NASA Nebula, "which started out as a Web consolidation exercise" [20],

(Continued)

[54] Examples include python (http://www.python.org/), Java (http://www.java.com), Springsource (http://www.springsource.com/), Apache Software Foundation (http://projects.apache.org/indexes/alpha.html), and Linux (http://kernel.org/).

[55] NASA Open Source Agreement (NOSA), which became the only government agency to receive OSI Certification. Available from: http://www.opensource.org/licenses/nasa1.3.

[56] Instead of using an existing licensing model, NASA chose to produce the NASA Open Source Agreement (NOSA), which became an OSI-approved software license.

[57] From NASA, The National Aeronautics Space Act [Internet]. Washington, DC: NASA [cited 2012 May 21]. Available from: http://www.nasa.gov/offices/ogc/about/space_act1.html. *"Provide for the widest practicable and appropriate dissemination of information concerning its activities and the results thereof."*

[58] A storefront portal hosted by GSA for federal agencies to find cloud computing applications to include business applications, productivity applications, cloud IT services, and social media apps.

[59] NASA Ames Research Center (ARC). Available from: http://www.nasa.gov/centers/ames/.

[60] From NASA, Nebula Cloud Computing Platform [Internet]. California: NASA Ames Research Center [cited 2011 November 11]. Available from: http://nebula.nasa.gov. *"Nebula is an open-source cloud computing project and service developed to provide an alternative to the costly construction of additional data centers."*

succeeded primarily because of the experience obtained through NASA's involvement in OSS.[61] Following experimentation with both commercial and open source cloud computing solutions, the Nebula project initiated an effort to begin building the first open source Infrastructure as a Service (IaaS) cloud software platform.[62] Nebula provided a case study for demonstrating the value OSS brought to the federal government.[63]

technologies leverage virtualization to support the ability to consolidate and improve government-wide IT utilization through shared infrastructures. The Cloud First and Shared First policies were established to increase the return on investment (ROI) associated with the federal government's use of its IT investment. The optimization of IT investment requires the use of the economies of scale offered by cloud commuting and other shared service[64] platforms. By leveraging reuse offered by OSS and the consolidation of redundant missions, through cross-organizational cloud services, efficiency can be delivered through more "economical" and "shared" delivery service models. The Digital Government Strategy, as illustrated in Figure 3.2, reiterated the need to deliver more efficient customer-centric services at a lower cost point through technologies that support the *information*,[65]*platform*,[66] and *presentations*[67] layers. In addition, cloud computing and related technologies offer a shared

[61] From Cureton, L., Braun, B. NPR 22101C, Requirement Waiver in Support of Open Source Software Development. Washington, DC: NASA; 2010. *For example, in November 2010, the NASA Chief Information Officer (CIO) issued a request for a waiver to support the release of the Nebula software for development in a publicly accessible repository to accelerate development and leverage community expertise to produce higher quality software.*

[62] The NASA Nebula cloud fabric became the Nova fabric controller as the Compute component of the OpenStack™ cloud software. Available from: http://www.openstack.org.

[63] Available from: http://nebula.nasa.gov/blog/2009/11/16/lowering-barrier-open-source/. *"Lowering the barrier to open source."*

[64] From VanRoekel, V. Federal Information Technology Shared Services Strategy. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. *"An information technology function that is provided for consumption by multiple organizations within or between Federal Agencies."*

[65] From Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. *"The information layer contains digital information."*

[66] From Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. *The platform layer includes all the systems and process to manage digital information.*

[67] From Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. *"The presentation layer defines the manager in which information is organized and provided to customers."*

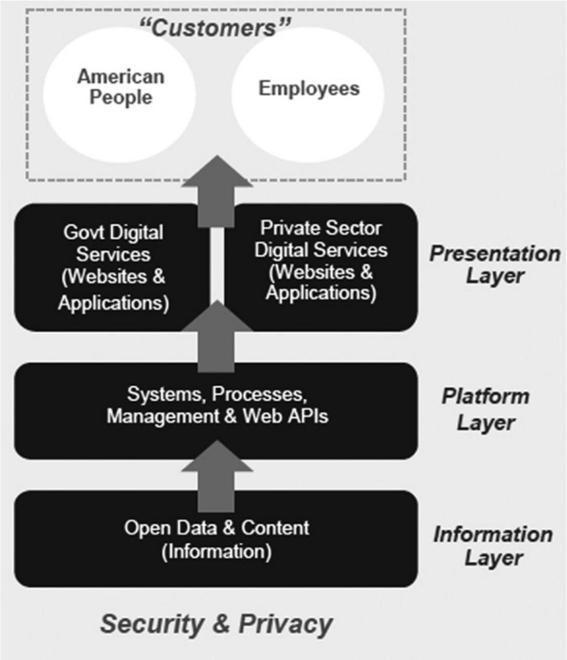

"Customers"
American People
Employees
Govt Digital Services (Websites & Applications)
Private Sector Digital Services (Websites & Applications)
Presentation Layer
Systems, Processes, Management & Web APIs
Platform Layer
Open Data & Content (Information)
Information Layer
Security & Privacy

FIGURE 3.2 Conceptual Layers of Digital Services [22]

platform to support the federal government's ability to manage information[68] in an organized manner and deliver the information using multiple accessibility modes (e.g., websites and mobile applications). A shared platform approach also provides an efficient and low-cost mechanism to develop and deliver services and information that support the strategy through three strategic objectives:

- Securely architect for interoperability and openness.
- Develop governance structure for digital services[69] (e.g., procurement and security policies and processes).
- Spur innovation by providing the federal government's data in open and machine-readable formats.

[68] From Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. *"Information, as defined in OMB Circular A-130, is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms."*

[69] From Office of Management and Budget (OMB). Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012. "*Digital services include the delivery of digital information (i.e., data or content) and transactional services (e.g.,online forms, benefits applications) across a variety of platforms, devices and delivery mechanisms (e.g.,websites, mobile applications, and social media).*"

OSS, as an enabler for cloud computing and other shared platforms, has accelerated the shift in technology delivery models, both in the public and private sectors. OSS has also produced many of the key technology innovations that are built into the foundation of this technology shift, such as different virtualization[70] technologies and cloud computing[71] platforms. These technologies and platforms can be leveraged to support the federal government's digital strategy through an open, standards-based approach that provides a more efficient use of rapidly evolving technologies. In addition, many OSS projects utilize a shared development methodology. This methodology promotes agility by bringing together a community of developers that can deliver innovative solutions faster and with fewer dedicated resources.

SUMMARY

In this chapter a case for open source was presented with a focus on understanding how the accelerated pathway to the cloud was, in part, contributed to by the broader government-wide acceptance of OSS. Challenges faced by the federal government in addressing acquisition were examined, which included licensing and federal procurement policies. Security was also discussed with specific focus on the processes and certification methods that provide risk-based approaches to verify OSS as part of the system development life cycle (SDLC). Finally, the chapter concluded with a brief discussion on how OSS is an enabler that supports the federal government's objectives of embracing technologies to promote efficiency and improved service delivery in a secure, standards-based approach.

References

[1] US House of Representatives. Subcommittee on oversight and investigation of the committee on Veteran's affairs [Internet]. Washington: US Government Printing Office [cited May 22, 2012]. <http://veterans.house.gov/sites/republicans.veterans.house.gov/files/documents/112-12transcripto-i5-11-11.html>.

[2] US Department of Veterans Affairs. VA launches open source custodian: open source electronics health record agent begins operations [Internet]. Washington: US Department of Veterans Affairs [cited May 22, 2012]. <http://www.va.gov/opa/pressrel/pressrelease.cfm?id=2153>.

[3] NASA. NASA clears the runway for open source software [Internet]. Washington, DC: National Aeronautics and Space Administration [cited May 24, 2012]. <http://www.nasa.gov/home/hqnews/2012/jan/HQ_12-021_Open_Source_Software.html>.

[70] Examples include Kernel-based Virtual Machine (http://www.linux-kvm.org/page/Main_Page) and Xen Hypervisor (http://xen.org/products/xenhyp.html).

[71] Examples include OpenStack™ cloud software (http://www.openstack.org) and CloudStack (http://cloudstack.org/).

[4] Evans K, Burton A. Office of Management and Budget (OMB) memorandum 04-16, software acquisition. Washington, DC: Executive Office of the President, Office of Management and Budget; 2004.

[5] President's Information Technology Advisory Committee. Developing open source software to advance high end computing. Washington, DC: National Coordination Office for Networking and Information Technology Research and Development; 2000.

[6] President's Information Technology Advisory Committee Letter [Internet]. Washington, DC: National Coordination Office for Networking and Information Technology Research and Development [cited October 20, 2011]. <http://www.nitrd.gov/Pitac/letters/pitac_ltr_sep11.html>.

[7] Stenbit DJ. Open source software (OSS) in the Department of Defense (DoD). Washington, DC: Department of Defense; 2003.

[8] Wennergren D. Clarifying guidance regarding open source software (OSS). Washington, DC: Department of Defense; 2009.

[9] Orszag P. Office of Management and Budget (OMB) Memorandum 10-06, Open Government Directive. Washington, DC: Executive Office of the President, Office of Management and Budget; 2009.

[10] The White House. Digital government: building a 21st century platform to better serve the American people. Washington, DC. Executive Office of the President, Office of Management and Budget; 2012.

[11] Streaming at 1:00 in the cloud [Internet]. Washington, DC: Office of Social Innovation and Civic Participation [cited November 2, 2011]. <http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud>.

[12] President's Information Technology Advisory Committee. Developing open source software to advance high end computing. Washington: National Coordination Office for Networking and Information Technology Research and Development; 2000.

[13] US Department of Defense (DoD), Chief Information Officer (CIO). [Internet]. Washington, DC: US Department of Defense [cited October 31, 2011]. http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx.

[14] US Department of Defense (DoD), Chief Information Officer (CIO). What license should the government or contractor choose/select when releasing open source software? [Internet]. Washington: US Department of Defense [cited June 2012]. <http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx#Q:_What_license_should_the_government_or_contractor_choose.2Fselect_when_releasing_open_source_software.3F>.

[15] US Department of Defense (DoD), Chief Information Officer (CIO). DoD open source software (OSS) FAQ [Internet]. Washington: US Department of Defense [cited June 2012]. <http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx> .

[16] CENDI Copyright Working Group. Frequently asked questions about copyright and computer software: issues affecting the US government with special emphasis on open source software. Tennessee: CENDI Secretariat; 2010.

[17] DHS Homeland Open Security Technology (HOST) [Internet]. Washington: US Government Printing Office [cited November 5, 2011]. <http://www.cyber.st.dhs.gov/host>.

[18] Stanford University. AFRL-RI-RS-TR-2009-192, Final technical report: the open source hardening project. New York: Air Force Research Laboratory; 2009.

[19] Moran P. Developing an open source option for NASA software. California: NASA Ames Research Center; 2003.

[20] Williams J. NASA Nebula in action: cloud computing case examples. California: NASA Ames Research Center; 2009.

[21] Kundra V. Federal cloud computing strategy. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.

[22] Office of Management and Budget (OMB) . Digital Government: Building a 21st Century Platform to Better Serve the American People. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012.

CHAPTER

Security and Privacy in Public Cloud Computing

4

INFORMATION IN THIS CHAPTER:

- Introduction
- Security and Privacy in the Context of the Public Cloud
- Federal Privacy Laws and Policies
- Safeguarding Privacy Information
- Security and Privacy Issues

INTRODUCTION

We have already learned in Chapter 1 that public cloud computing presents the federal government with significant opportunities for reduced cost and improved operational efficiency. In this chapter, the discussion will focus specifically on security and privacy within the context of public cloud computing. Public cloud services can provide benefits for improved information security, and even enhance privacy practices. But the benefits of public cloud computing can be outweighed by potential security and privacy issues, concerns, or risks[1] if there is not a comprehensive "due diligence" process. The due diligence process helps ensure the issues, concerns, or risks are integrated into the preliminary cloud service selection and assessment activities.

Security and privacy are distinct and independent disciplines in which aspects of privacy, as will be discussed later in this chapter, include specific principles and considerations that do not necessarily overlap with security. But foundational security practices are required for privacy to be effective in a public cloud computing environment. Therefore, the information that will be hosted within a public cloud service needs to be designed and operate to meet the same security and privacy requirements

[1] The European Network and Information Security Agency (ENISA), *Cloud Computing: Benefits, risks and recommendation for information security* provides a list of 35 risks that cover areas such as policy and organizational, technical, legal, and traditional IT. Available from: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00004-6

The Federal Cloud Computing Strategy [1] highlighted several potential security benefits that can be achieved through the use of cloud services, to include:

- *Staff specialization*—the ability to focus resources on areas of high concern as more general security services are assumed by the cloud provider.
- *Platform strength*—potential platform strength resulting from greater uniformity and homogeneity, and resulting improved information assurance, security response, system management, reliability, and maintainability.
- *Resource availability*—improved resource availability through scalability, redundancy, and disaster recovery capabilities; improved resilience to unanticipated service demands.
- *Backup and recovery*—improved backup and recovery capabilities, policies, procedures, and consistency.
- *Data concentration*—ability to leverage alternate cloud service to improve the overall security posture than that of traditional data centers.

as traditional federal information systems. Federal agencies will likely base their analysis in the context of their own use cases[2] for a public cloud service to ensure the Cloud Service Provider (CSP) has addressed all applicable laws, regulations, and policies. Their analysis could leverage existing practices when considering general security and privacy issues (e.g., data location, data ownership, risk, visibility, etc.) for privacy-related information that will be stored, processed, or transmitted through the use of public cloud services.

The transition to a public cloud service requires federal agencies and CSPs to review their governance practices (i.e., policies, procedures, and processes) to ensure from an organizational perspective the existing roles and responsibilities can operate effectively in the context of privacy. Federal agencies may also have to introduce new risk management[3] processes. Risk assessments performed in a traditional computing environment where the federal agency has more control over the risks mitigations may not be possible to achieve within a public cloud service, and will instead require a close coordination with the CSP to ensure mitigations are appropriately integrated and managed. Therefore, the consistency between the federal agencies' and the CSPs' risk management process is essential to ensure risks identified are adequately prioritized and mitigated through the selection and implementation of security

[2] From National Institute of Standards and Technology (NIST). Cloud Computing Business Use Cases Working Group [Internet]. Maryland: National Institute of Standards and Technology [cited 2011 Aug 22]. Available from: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/BusinessUseCases. *The NIST CC Business Use Cases Working Group consists of federal agencies and industry to define target USG Cloud Computing business use cases (set of candidate deployments to be used as examples) for Cloud Computing model options, to identify specific risks, concerns and constraints.*

[3] From Kundra, V. *Federal Cloud Computing Strategy*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. *"Risk management entails identifying and assessing risk, and taking the steps to reduce it to an acceptable level."*

controls that minimize the “significant privacy concerns associated with the [public] cloud computing environment” [2].

The Federal Risk and Authorization Management Program (FedRAMP),[4] which will be discussed in more detail in later chapters, provides a common framework that uses existing processes and practices already used by federal agencies to verify the security and privacy requirements.[5] For example, a Privacy Impact Assessment (PIA)[6] is a tool already required by federal agencies[7] and is used to determine the type of privacy-related information stored, processed, or transmitted through the use of the target public cloud computing environment. In addition, the PIA helps guide the determination of the types of protections that are required for selecting appropriate security and privacy controls that need to be implemented by CSPs to adequately mitigate identified risks to privacy information. In addition, the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP)[8] can be used by federal agencies (and CSPs) in the context of public cloud computing to address the identification of information security and data privacy requirements [3].

SECURITY AND PRIVACY IN THE CONTEXT OF THE PUBLIC CLOUD

Public cloud computing by definition is a service that is owned, managed, and operated by a service provider (e.g., private company, federal or state government, etc.) on its premises and is consumed by the general public [5]. Cloud computing delivery models are comparably different from what is commonly used by many federal agencies where their information systems are hosted within traditional, dedicated infrastructures located within a federal data center or in a contractor’s data center. New types of technologies and delivery models will likely introduce new definitions, making it difficult and important to have a common context[9] for federal agencies to use

[4] The Federal Risk and Authorization Management Program (FedRAMP) is discussed in detail in Chapter 8, FedRAMP Primer, and Chapter 9, The FedRAMP Cloud Computing Security Requirements.

[5] Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA). Available from: http://www.gsa.gov/graphics/staffoffices/PTA_and_PIA_050212_508.doc.

[6] From McCallister, E., Grance, T., Scarfone, K. NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Maryland: National Institute of Standards and Technology; 2010. *“A structured process for identifying and mitigating privacy risks.”*

[7] Office of Management and Budget (OMB) Memorandum 03-22 (M-03-22), *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. Available from: http://www.whitehouse.gov/omb/memoranda_m03-22.

[8] The Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) is a common language that can be used when discussing security and privacy in the context of the organization’s mission and integration into business processes.

[9] Conditions (or facts) about the environment [i.e., public cloud] in which something [i.e., privacy information] exists (or resides).

when determining how the public cloud service will be used to store, process, or transmit sensitive data collected to support their mission and business requirements.

For the purpose of this chapter, the NIST definition provides a good starting point for discussing security and privacy issues in public cloud computing. The basic characterization by NIST of public cloud computing only intended to serve as a means for a broad comparison [4]. This definition is supported by a conceptual reference architecture, depicted in Figure 4.1, (and taxonomy) that provides a high-level illustration of security and privacy as cross-cutting and existing across all architectural layers.

In addition, the conceptual reference architecture provides a useful tool for focusing on the security and privacy requirements for what CSPs need to provide rather than describing a specific solution that needs to be designed and implemented [5]. When federal agencies begin to plan for security and privacy considerations in public cloud services, the generalization of the NIST definition can be further expanded to include a definition of specific security and privacy security requirements. This elaboration of the basic NIST definition enables the selection of a common group of public cloud services based on an examination of the context given by the federal agency's requirements. In contrast, the CSP can perform a similar activity by identifying a target group of federal agencies, and reflect their requirements in the context of their cloud service to determine if any additional security and privacy controls need to be applied to make it acceptable for use.

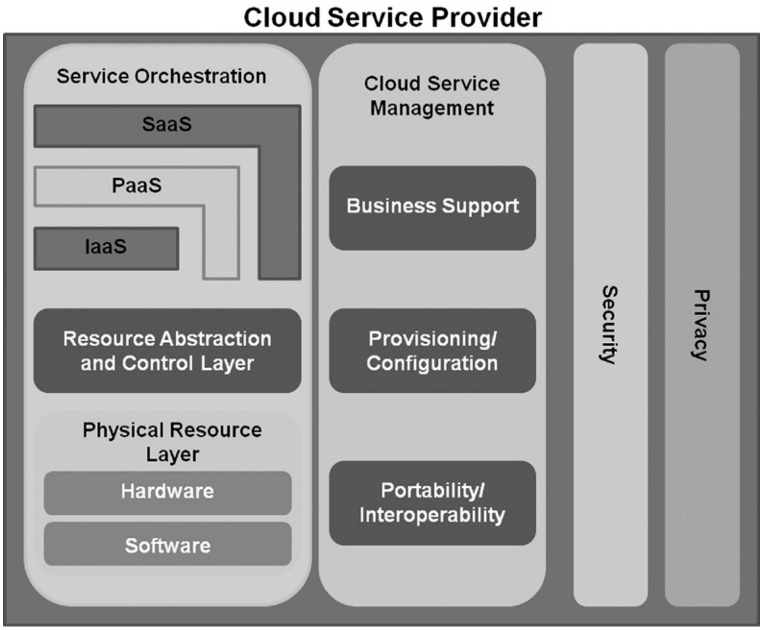


FIGURE 4.1 Conceptual Reference Model—Cross-Cutting Security and Privacy

TIP

The Federal Cloud Computing Strategy [1] identified several key security considerations to guide federal agencies in assessing the risk in the context of the public cloud computing environment and improve confidence in the use of cloud services:

- carefully define security and privacy requirements during the initial planning stage at the start of the systems development life cycle;
- determine the extent to which negotiated service agreements are required to satisfy security requirements; and the alternatives of using negotiated service agreements or cloud computing deployment models which offer greater oversight and control over security and privacy;
- assess the extent to which the server and client-side computing environment meets organizational security and privacy requirements; and
- continue to maintain security management practices, controls, and accountability over the privacy and security of data and applications.

WARNING

Federal agencies are obligated through the Federal Information Security Management Act (FISMA) with a number of requirements that include, although not specifically limited to, OMB policies, FIPS standards, federal agency-specific policy requirements and authorization, and continuous monitoring requirements. Therefore, when federal agencies make the decision to choose a public cloud service for their agencies' outsourcing needs, they have been encouraged to carefully consider the following types of factors:

- *statutory compliance* (laws, regulations, and agency requirements);
- *data characteristics* (fundamental protections an application's data set requires);
- *privacy and confidentiality* (protect against accidental and nefarious access to information);
- *integrity* (ensure data is authorized, complete, and accurate);
- *data controls and access policies* (where data can be stored and who can access physical locations); and
- *governance* (ensure that cloud computing service providers are sufficiently transparent, have adequate security and management controls, and provide the information necessary for the agency to appropriately and independently assess and monitor the efficacy of those controls) [1].

FEDERAL PRIVACY LAWS AND POLICIES

Privacy is a core value of American society. The importance of protecting privacy information is already a part of many industries in which US federal privacy laws span. Table 4.1 provides an example of some of the types of regulatory and legislative frameworks that exist that might be relevant when considering the collection and storage of privacy-related information in a public cloud service.

In 1972, the Secretary of Health, Education, and Welfare (HW) formed the *Advisory Committee on Automated Personal Data Systems,* "to analyze the consequences of using computers to keep records about people" [7]. The committee produced a report in which it was concluded that "safeguards for personal privacy based on our

Table 4.1 Coverage of Existing US Federal Privacy Laws [6]

Industry	Regulatory and Legislative Frameworks
Healthcare	Health Insurance, Portability and Accountability Act (HIPAA) and the associated Health Information Technology for Economic and Clinical Health (HITECH) Act
Financial	Gramm-Leach-Bliley (GLBA), the Fair and Accurate Credit Transaction Act (FACTA), and the Red Flags Rule
Education	Family Education Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA)
Communications	First Amendment to the US Constitution, the Electronic Communications Privacy Act (ECPA), and the Telephone Consumer Protection Act (TCPA)
Government	Privacy Act of 1974, the Computer Security Act of 1987, and the E-Government Act of 2002
Employee and Labor Laws	Americans with Disability Act (ADA) and the Equal Employment Opportunity (EEO) Act

concept of mutuality in record-keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice" [7]. The report recommended the adoption of a federal Code of Fair Information Practices (FIPs)[10] for the protection of information within computers [referred to as automated personal data systems]. In 1980, the Organization for Economic Cooperation and Development (OECD) revised and adopted the original FIPs and extended them to create a set of eight Fair Information Practice Principles (FIPPs)[11] listed in Table 4.2.

Many of the US privacy laws are based on the FIPPs as an industry recognized a set of practices for protecting data and privacy.

The federal government has the legal responsibility to ensure governance and accountability of personally identifiable information (PII).[12] Safeguarding PII in the possession of the federal government and preventing its breach are essential to ensure the trust of the American public [9]. Therefore, before we can effectively discuss potential security and privacy issues, a basic understanding is required of some of the

[10] The Code of Fair Information Practices, now known as the Fair Information Practices Principles, included five principles. Available from: http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[11] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Available from: http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[12] From McCallister, E., Grance, T., Scarfone, K. NIST Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Maryland: National Institute of Standards and Technology; 2010. *"Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal law."*

Table 4.2 Fair Information Practice Principles (FIPPs) [8]

FIPPs	Description
Collection Limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject
Data Quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date
Purpose Specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose
Use Limitation	Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law
Security Safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data
Openness	There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller
Individual Participation	An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended
Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above

significant privacy laws and policies developed for the protection and preservation of privacy rights of individuals by federal agencies.

Privacy Act of 1974

The Privacy Act of 1974[13] was established as a statutory framework to govern the federal government's collection and use of personal information. This statutory

[13] *The Pivacy Act of 1974 (Public Law 93-579)*. Available from: http://www.justice.gov/opcl/privstat.htm.

framework balances the federal government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from the collection, maintenance, use, and disclosure of personal information about them [10].

The Privacy Act is based on the internationally recognized FIPPs previously discussed. The Act protects certain federal government records[14] pertaining to individuals,[15] collected, maintained, used, and disseminated by federal agencies. The records containing PII are stored in a system of records (SOR) which is "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" [11].

In accordance with the Privacy Act,[16] federal agencies are required to give public notice through a Systems of Records Notice (SORN) in the Federal Registrar,[17] that includes information about the SOR such as

- System name.
- Security classification.
- System location(s).[18]
- Categories of individual covered by the system.
- Categories of records covered by the system.
- Authority for maintenance of the system.
- Disclosure to consumer reporting agencies.
- Routine use of records maintained in the system, including categories of users and the purpose of such uses.
- Policies and practices for storing, retrieving, access, retaining, and disposal of records in the system.
- Exceptions claimed for the system.

[14] From Office of Management and Budget (OMB). Privacy Act Implementation: Guidelines and Responsibilities. Washington, DC: Executive Office of the President, Office of Management and Budget; 1975. "*The term* "*record*" *means any item, collection, or grouping of information about an individual that is maintained by an agency.*"

[15] From Office of Management and Budget (OMB). Privacy Act Implementation: Guidelines and Responsibilities. Washington, DC: Executive Office of the President, Office of Management and Budget; 1975. "*The term* "*individual*" *means a citizen of the United States or an alien lawfully admitted for permanent residence.*"

[16] U.S.C. section 552a – Records maintained individuals.

[17] From The Federal Register [Internet]. Washington, US: Government Printing Office [cited 2011 Sep 31]. Available from: http://www.gpo.gov/help/about_federal_register.htm. *"The Federal Register is the official daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as executive orders and other presidential documents."*

[18] From Federal CIO Council and Chief Acquisition Officers Council. Creating Effective Cloud Computing Contracts for the Federal Government. Washington: Executive Office of the President, Office of Management and Budget; 2012. "Under the Privacy Act, Federal agencies must be able to inform individuals, in the applicable SORN, where their data is being maintained, which can be complicated in a CSP environment."

TIP

Under Section (m) of the Privacy Act, a government contractor's information system is subject to the requirements of the Act, if under contract, the federal agency contracts for the operation by or on behalf of the agency, a SOR to accomplish an agency function [11]. Since CSPs may store records covered under the Privacy Act, the CSPs' cloud service could be considered a SOR and be subject to the same requirements[19] as federal agencies. In addition, a cloud service operated by a CSP that is covered by the Privacy Act could be subject to civil and criminal implications if the CSP knowingly and willfully acts or fails to act as described in the Privacy Act [21].

NOTE

The Privacy Act Issuances[20]

According to the Privacy Act, the Office of the Federal Register (OFR) must biennially compile and publish (1) descriptions of system of records maintained on individuals by federal agencies which were published in the Federal Register; and (2) rules of each agency which set out the procedures agencies will follow in helping individuals who request information about their records. In addition, the Privacy Act requires OFR to publish the compilation in a form available to the public at a low cost [12].

The extension of Privacy Act requirements for the collection and storage of PII to a public cloud service will likely need to be carefully evaluated by the CSP and the federal agency for a cloud service operating as the federal agencies' SOR. "Once an agency chooses a cloud computing provider to collect and store information, the individual is no longer providing information solely to the government, but also to a third party who is not necessarily bound by the same laws and regulations" [13]. Since federal agencies are "ultimately accountable for the security and privacy of data held by a cloud provider on their behalf" [5], the requirements of the Privacy Act and the responsibility for the implementation of privacy controls will be discussed later in this chapter. Therefore, assistance or requirements by the CSP to support the federal agency meeting requirements under the Privacy Act will need to be clearly addressed through a contractual obligation (e.g., protecting privacy information, and reporting breaches or disclosures).

E-Government Act of 2002, Federal Information Security Management Act (FISMA)

FISMA provides federal agencies with a recommended set of security control requirements[21] necessary to protect information contained within an information

[19] Government contractors fall under subsection (m) of the Privacy Act of 1974.

[20] Privacy Act Issuances. Available from: http://www.ofr.gov/privacy/AGENCIES.aspx.

[21] From E-Government Act of 2002 [Internet]. Washington: US Government Printing Office [cited 2011 Oct 9]. Available from: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm. *Comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.*

system.[22] In addition, federal agencies are required to identify and assess the risk to their PII, and to ensure security controls are implemented to enable adequate security. Therefore, CSPs that collect, store, or process PII on behalf of the federal government may have a responsibility to meet specific security requirements. These security requirements are based on the confidentiality,[23] integrity, and available objectives for the information identified as a result of a security categorization conducted by the CSP or the federal agency.

NIST was given the responsibility for developing standards and guidelines for information systems. These standards and guidelines include providing federal agencies with guidance[24] on categorizing PII. The Privacy Act requires federal agencies to establish administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenient or unfairness on whom information is obtained [9]. Harm is the adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII [14]. Therefore, the loss (or breach) of confidentiality would likely need to be evaluated against the unauthorized disclosure of the PII and the "effect on the organizational operations, organizational assets, or individual" [15] against the different confidentiality impact levels (see Table 4.3).

FISMA also required federal agencies to establish procedures for the detection, reporting, and response of security incidents. In addition, OMB requires federal agencies to report incidents involving PII to the US Department of Homeland Security (DHS), US Computer Emergency Readiness Team (US-CERT).[25] Incidents that involve breaches to PII are categorized by the US-CERT as a Category 1 and require reporting within one hour of the discovery/detection. The CSPs' incident response plan[26] will need to reflect any new requirements for notification and reporting by ensuring service agreements address the requirements and responsibility for notification, reporting, and any costs associated with an incident involving the compromise of PII.

[22] From Office of Management and Budget (OMB), OMB Circular No. A-130 Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources. Washington, DC: Executive Office of the President, Office of Management and Budget; 2000. "*A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual*."

[23] US Congress. Federal Information Security Management Act. Washington, DC: US Congress; 2002. "*Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information*."

[24] Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Available from: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[25] US-CERT Incident Reporting System. Available from: https://forms.us-cert.gov/report/.

[26] NIST Special Publication (SP) 800-61 Revision 2, Computer Security Incident Handling Guide. Available from http://csrc.nist.gov/publications/nistpubs/SP800-61rev2/SP800-61rev2.pdf.

Table 4.3 FIPS 199 Impact Level—Confidentiality [15]

Potential Impact	Potential Impact
Low	The unauthorized disclosure of information could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals
Moderate	The unauthorized disclosure of information could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals
High	The unauthorized disclosure of information could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals

OMB Memorandum Policies

PII refers to information that can be used to distinguish[27] or trace[28] an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked[29] or linkable[30] to a specific individual, such as date and place of birth, mother's maiden name, etc. [9].

PII can include the following types of information:

- Name.
- Social Security number.
- Date and place of birth.
- Mother's maiden name.
- Biometric records.
- Education.
- Financial transactions.
- Medical history.

[27] From McCallister, E., Grance, T., Scarfone, K. NIST Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Maryland: National Institute of Standards and Technology; 2010. "*To identify an individual.*"

[28] From McCallister, E., Grance, T., Scarfone, K. NIST Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Maryland: National Institute of Standards and Technology; 2010. *"Process sufficient information to make a determination about a specific aspect of an individual's activities or status."*

[29] From McCallister, E., Grance, T., Scarfone, K. NIST Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Maryland: National Institute of Standards and Technology; 2010 "*Information about or related to an individual that is logically associated with other information about the individual.*"

[30] From McCallister, E., Grance, T., Scarfone, K. NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Maryland: National Institute of Standards and Technology; 2010 "*Information about or related to an individual that is logically associated with other information about the individual.*"

- Criminal or employment history and information which can be used to distinguish or trace an individual's identity.

OMB has established a number of governing policies for federal agencies relating to PII over the years. Table 4.4 provides a list of applicable privacy-related policies that must be adhered to by federal agencies.

SAFEGUARDING PRIVACY INFORMATION

Privacy and security can mean different things to different people because they are identified as distinct disciplines. Privacy and security do overlap in many aspects, but privacy includes more than security and confidentiality and includes the principles of transparency and notice and choice [16]. However, it is widely agreed upon that

Table 4.4 Federal Privacy Related Policies

Government-wide Policy	Description
OMB Circular A-130, Management of Federal Information Resources, Appendix I	This appendix describes agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974, 5 U.S.C. 552a, as amended (hereinafter "the Act"). It applies to all agencies subject to the Act. Note that this Appendix does not rescind other guidance OMB has issued to help agencies interpret the Privacy Act's provisions, e.g., Privacy Act Guidelines (40 FR 28949–28978, July 9, 1975), or Final Guidance for Conducting Matching Programs (54 FR at 25819, June 19, 1989)
OMB Memo M-99-18, Privacy Policies on Federal Web Sites	This memorandum directs departments and agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so
OMB Memo M-03-22, OMB Guidance for Implementing the Privacy Provisions	The memorandum provides guidance to agencies on implementing the privacy provisions of the E-Government Act of 2002
OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of PII	The memorandum reemphasizes the responsibilities under existing law, executive orders, regulations, and policy to appropriately safeguard personally identifiable information and train employees on responsibilities in this area. It also establishes additional privacy and security requirements
OMB Memo M-10-23, Guidance for Agency Use of Third-Party Websites	This memorandum requires federal agencies to take specific steps to protect individual privacy whenever they use third-party websites and applications to engage with the public

some aspects of privacy require a sound security practice (e.g., accountability, integrity, confidentiality, and data destruction). Therefore, it is important to recognize that "organizations cannot have effective privacy without a solid foundation of information security" [16].

Privacy can be summarized as the need to protect certain information about individuals and organizations and "involves the right to control when, where, how, to whom, and to what extent an individual shares their own personal information, as well as the right to access personal information given to others, to correct it, and to ensure it is safeguarded and disposed of appropriately" [6]. Security, on the other hand, provides the safeguards (e.g., administrative, technical, and physical) for achieving the confidentiality, integrity, and availability objectives for protecting the privacy information.

Confidentiality refers to what data may be disclosed and to whom the data may be disclosed, thereby ensuring that only legally authorized and appropriate disclosures are made. Integrity is the assurance that information and information systems are protected against improper or accidental modification. Availability is the assurance of timely and reliable access to information and information systems by authorized persons [17]. Figure 4.2 provides an illustration that depicts the relationship that exists between privacy (FIPPs) as and security (Safeguards) and which might require implementation within a public cloud computing environment

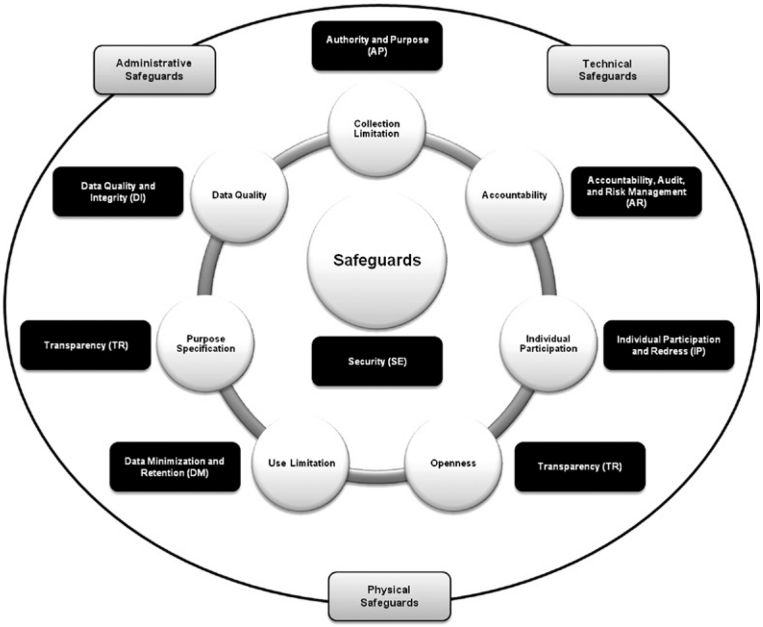


FIGURE 4.2 Relationship between FIPPs and Safeguards

to prevent the unauthorized access, use, disclosure, modification, and destruction of PII.

As we already discussed, FIPPs provide an internationally accepted framework, reflected in many US laws for addressing privacy requirements. FIPPs also serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies [16].

NIST and the Federal CIO Council's Privacy Committee developed a comprehensive set of privacy controls[31] for federal agencies to use for ensuring they develop and implement appropriate privacy protection and practices to achieve the organization's privacy objectives. Privacy controls[32] provide "a roadmap for organizations to use in identifying and implementing privacy controls concerning the life cycle of PII" [16] and when to "address potential risks when moving to a cloud computing environment" [18]. In addition, the privacy control can be used within existing federal government frameworks[33] such as the Federal Risk and Authorization Management Program (FedRAMP) when specifying the federal privacy requirements for government-wide use of public cloud services when privacy-related information is involved.

Privacy Controls

The privacy controls included in this section are based on those identified in the *Security and Privacy Controls for Federal Information Systems and Organizations*. Table 4.5 provides a description of each of the privacy control families. These privacy controls provide the safeguards (i.e., administrative, technical, and physical) to be implemented by the CSP or within the public cloud service when it has been determined PII is being collected and stored.

[31] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2011. *The privacy controls are based on the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act of 1974, Section 208 of the E- Government Act of 2002 and related Office of Management and Budget (OMB) guidance.*

[32] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. "*The Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) also provided information and materials in development of the privacy controls.*"

[33] From Federal Chief Information Officers Council, Privacy Committee, Web 2.0/Cloud Computing Subcommittee. Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010. *In August of 2010, the Federal CIO published as a framework that addresses privacy considerations posed by moving computer systems that contain PII to a Cloud Computing Provider (CCP).*

Table 4.5 Summary of Privacy Control Families [16]

Control Family	Description
Authority and Purpose (AP)	This family furthers compliance with the Privacy Act by ensuring that organizations: (i) identify the legal bases that authorize a particular PII collection or activity that impacts privacy; and (ii) specify in their notices, the purpose(s) for which PII is collected
Accountability, Audit, and Risk Management (AR)	This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk
Data Quality and Integrity (DI)	This family ensures compliance with Section 552a (e)(2) of the Privacy Act of 1974 and enhances public confidence that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices
Data Minimization and Retention (DM)	This family helps organizations implement the data minimization and retention elements of the Privacy Act, which requires organizations to collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. Organizations retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule
Individual Participation and Redress (IP)	This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII, as required by the Privacy Act. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII
Security (SE)	This family supplements the security controls in Appendix F to ensure administrative, technical, and physical safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework
Transparency (TR)	This family implements Sections 552a (e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act, which require public notice of an organization's information practices and the privacy impact of government programs and activities
Use Limitation (UL)	This family helps organizations comply with the Privacy Act, which prohibits the use of PII that is either not specified in notices, incompatible with the specified purposes, or not otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

Authority and Purpose (AP)

AP-1	**Authority to Collect**
Control Requirement:	The organization determines the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A) Section 208(c). • E-Government Act of 2002 (P.L. 107-347).
AP-2	**Purpose Specification**
Control Requirement:	The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B); Sections 208(b), (c). • E-Government Act of 2002 (P.L. 107-347).

Accountability, Audit, and Risk Management (AR)

AR-1	**Governance and Privacy Program**
Control Requirement:	The organization: **a.** Appoints a Senior Agency Official for Privacy (SAOP)/ Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; **b.** Monitors federal privacy laws and policy for changes that affect the privacy program; **c.** Allocates [*Assignment: organization-defined allocation of budget and staffing resources*] to implement and operate the organization-wide privacy program; **d.** Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; **e.** Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and **f.** Updates privacy plan, policies, and procedures [*Assignment: organization-defined frequency, at least biennially*].

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

AR-1	**Governance and Privacy Program**
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a. • E-Government Act of 2002 (P.L. 107-347). • Federal Information Security Management Act of 2002 (FISMA) 44 U.S.C. § 3541. • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. • OMB Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*. • OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. • OMB Circular A-130, *Management of Federal Information Resources*. • Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP).
AR-2	**Privacy Impact and Risk Assessment**
Control Requirement:	The organization: **a.** Establishes a privacy risk assessment process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, and use of personally identifiable information (PII); **b.** Conducts a Privacy Impact Assessment (PIA) for information systems and programs in accordance with applicable law, OMB policy, and any existing organizational policies and procedures; and **c.** Follows a documented, repeatable process for conducting, reviewing, and approving PIAs.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208. • E-Government Act of 2002 (P.L. 107-347) • Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541; • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. • OMB Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*.

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

AR-3	**Privacy Requirements for Contractors and Service Providers**
Control Requirement:	The organization: **a.** Establishes privacy roles and responsibilities for contractors and service providers; and **b.** Includes privacy requirements in contracts and other acquisition-related documents.
References:	• OMB Circular A-130, *Management of Federal Information Resources*.
AR-4	**Privacy Monitoring and Auditing**
Control Requirement:	The organization monitors and audits privacy controls and internal privacy policy [*Assignment: organization-defined frequency*] to ensure effective implementation.
References:	• Section 208, E-Government Act of 2002 (P.L. 107-347); Federal Information Security. • Management Act of 2002 (FISMA), 44 U.S.C. § 3541 • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. • OMB Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*.
AR-5	**Privacy Awareness and Training**
Control Requirement:	The organization: **a.** Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; **b.** Administers basic privacy training *[Assignment:* organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [*Assignment*: organization-defined frequency, at least annually]; and **c.** Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [*Assignment:* organization-defined frequency, at least annually].
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208. • E-Government Act of 2002 (P.L. 107-347). • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. • OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

AR-6	**Privacy Reporting**
Control Requirement:	The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB) and Congress to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208. • E-Government Act of 2002 (P.L. 107-347). • Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541; Section 803. • 9/11 Commission Act, 42 U.S.C. § 2000ee-1; Section 804. • 9/11 Commission Act, 42 U.S.C. § 2000ee-3; Section 52. • Consolidated Appropriations Act of 2005 (P.L. 108-447). • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. • OMB Circular A-130, *Management of Federal Information Resources*.
AR-7	**Privacy-Enhanced System Design and Development**
Control Requirement:	The organization designs information systems to enhance privacy by automating privacy controls.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208 (b) and (c). • E-Government Act of 2002 (P.L. 107-347). • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
AR-8	**Accounting of Disclosures**
Control Requirement:	The organization, consistent with, and subject to exceptions in, the Privacy Act: **a.** Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: – Date, nature, and purpose of each disclosure of a record; and – Name and address of the person or agency to which the disclosure was made; **b.** Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and **c.** Makes the accounting of disclosures available to the person named in the record upon request.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (c).

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

Data Quality and Integrity (DI)

DI-1	**Data Quality**
Control Requirement:	The organization: **a.** Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; **b.** Collects PII directly from the individual to the greatest extent practicable; **c.** Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [*Assignment*: organization-defined frequency]; and **d.** Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e)(5). • Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4. • Paperwork Reduction Act, 44 U.S.C. § 3501. • OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001). • OMB Memorandum 07-16*, Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.
DI-2	**Data Integrity and Data Integrity Board**
Control Requirement:	The organization: **a.** Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and **b.** Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (u). • OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*.

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

Data Minimization and Retention (DM)

DM-1	**Minimization of Personally Identifiable Information**
Control Requirement:	The organization: **a.** Identifies the minimum personally identifiable information (PII) elements (e.g., name, address, date of birth) that are relevant and necessary to accomplish the legally authorized purpose of collection; **b.** Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and **c.** Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [*Assignment*: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (e)(2); Section 208(b). • E-Government Act of 2002 (P.L. 107-347) • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. • OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.
DM-2	**Data Retention and Disposal**
Control Requirement:	The organization: **a.** Retains personally identifiable information (PII) for [*Assignment*: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; **b.** Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and **c.** Uses [*Assignment: organization-defined techniques or methods*] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A); Section 208(c). • E-Government Act of 2002 (P.L. 107-347).

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

DM-3	**Minimization of PII Used in Testing, Training, and Research**
Control Requirement:	The organization: **a.** Develops policies and procedures for the use of personally identifiable information (PII) for testing, training, and research; and **b.** Implements controls to protect PII used for testing, training, and research.
References:	• NIST Special Publications 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.
Individual Participation and Redress (IP)	
IP-1	**Consent**
Control Requirement:	The organization: **a.** Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; **b.** Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; **c.** Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and **d.** Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A); Section 208(c). • E-Government Act of 2002 (P.L. 107-347). • NIST Special Publications 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

IP-2	**Individual Access**
Control Requirement:	The organization, consistent with, and subject to exceptions in, the Privacy Act: **a.** Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records in order to determine whether to have the PII corrected or amended, as appropriate; **b.** Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; **c.** Publishes access procedures in System of Records Notices (SORNs); and **d.** Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (d). • OMB Circular A-130, *Management of Federal Information Resources*.
IP-3	**Redress**
Control Requirement:	The organization: **a.** Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and **b.** Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (d). • OMB Circular A-130, *Management of Federal Information Resources.*
IP-4	**Complaint Management**
Control Requirement:	The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.
References:	• OMB Circular A-130, *Management of Federal Information Resource*. • OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. • OMB Memorandum 08-09, *New FISMA Privacy Reporting Requirements for FY 2008*.

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

Security (SE)

SE-1	**Authority to Collect**
Control Requirement:	The organization: **a.** Establishes, maintains, and updates [*Assignment*: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and **b.** Provides each update of the PII inventory to the CIO or information security official [*Assignment*: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2). • E-Government Act of 2002 (P.L. 107-347). • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. • OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*. • FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. • NIST Special Publications 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. • NIST Special Publications 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*.
SE-2	**Privacy Incident Response**
Control Requirement:	The organization: **a.** Develops and implements a Privacy Incident Response Plan; and **b.** Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m). • Federal Information Security Management Act of 2002 (FISMA) 44 U.S.C. § 3541. • OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*. • OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. • NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

Transparency (TR)

TR-1	**Privacy Notice**
Control Requirement:	The organization: **a.** Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; **b.** Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII for the purpose of having it amended or corrected, where appropriate; and (vi) how the PII will be protected; and **c.** Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b). • E-Government Act of 2002 (P.L. 107-347). • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. • OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. • OMB Memorandum 10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*. • OMB Memorandum 10-23, *Guidance for Agency Use of Third-Party Websites and Applications*. • ISE Privacy Guidelines[a]

[a] *ISE Privacy Guidelines. Available from: http://ise.gov/ise-privacy-guidelines*

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

TR-2	**Authority to Collect**
Control Requirement:	The organization, consistent with the Privacy Act: **a.** Publishes in the Federal Register, System of Records Notices (SORNs) for information systems containing personally identifiable information (PII); **b.** Keeps SORNs current; and **c.** Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.
References:	• The Privacy Act of 1974, 5 U.S.C. § e(3). • OMB Circular A-130, *Management of Federal Information Resources*.
TR-3	**Dissemination of Privacy Program Information**
Control Requirement:	The organization: **a.** Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and **b.** Ensures that its privacy practices are publicly available through organizational websites or otherwise.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208. • E-Government Act of 2002 (P.L. 107-347). • OMB Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
Use Limitation (UL)	
UL-1	**Internal Use**
Control Requirement:	The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b)(1).

Table 4.5 Summary of Privacy Control Families [16] (*Continued*)

UL-2	**Information Sharing with Third Parties**
Control Requirement:	The organization: **a.** Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or in a manner compatible with those purposes; **b.** Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;, **c.** Monitors, audits, and trains its staff on the authorized uses and sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and **d.** Evaluates any proposed new instances of sharing PII with third parties to assess whether they are authorized and whether additional or new public notice is required.
References:	• The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o). • ISE Privacy Guidelines.

Data Breaches, Impacts, and Consequences

Data breaches[34] involving PII extend beyond the individual[35] (e.g., identity theft[36]) involved and can produce significant impacts for the CSP and/or the federal agency. The organizational impacts can include lost revenue and unbudgeted costs associated

[34] From Wood, D. GAO Report 07-737, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown. Washington: US General Accountability Office; 2007. *"An organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers."*

[35] The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer organization which seeks to raise consumers' awareness of how technology affects personal privacy, and to document privacy complaints. The PRC maintains the Chronology of Data Breaches located at http://www.privacyrights.org/data-breach.

[36] *Federal Identity Theft Laws*. Available from: http://www.ojp.usdoj.gov/ovc/pubs/ID_theft/idtheft-laws.html.

NOTE

On May 10, 2006, Executive Order 13402, "*Strengthening Federal Efforts to Protect Against Identity Theft*," was issued to create a Presidential Identity Theft Task Force to review and advise on the execution of the policy[37] set forth by the President of the United States for "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information.*" As a result of the Task Force, OMB issued a policy reiterating the privacy and security requirements for federal agencies under the Privacy Act (and other laws, executive orders, regulations, and policies), and required federal agencies to develop and implement breach notification policies.

In addition, it highlighted new technical controls that were to supplement those already required under US laws and policies. For example, OMB established additional security requirements for the protection of all federal information (regardless of whether it was covered under the Privacy Act). These security requirements included:

- encryption using NIST-certified cryptographic modules[38] to mobile computers/devices,
- two-factor authentication for remote access,
- enforcement of a "time-out" capability requiring re-authentication after 30 minutes of inactivity, and
- logging and verification of all data extracts from database containing sensitive information, including the verification of destruction after 90 days (if no longer being used).

with responding to the incident, or even a loss of credibility, confidence, and trust from existing customers or the public.

Data breaches can also occur for a variety of reasons. Some occur due to intentional actions such as theft of information; others are due to negligence or accidents. Intentional actions involve breaches such as hacking, employee theft, theft of physical equipment, or deception or misrepresentation to obtain unauthorized data. Negligence or accidental losses include loss of laptop computer or other hardware, loss of data tapes, unintentional exposure on the Internet, or improper disposal of data [19].

Consequences and accountability are important aspects to ensure compliance with federal privacy laws and policies that lead to the adequate handling and safeguarding of PII. To address this necessity, OMB requires federal agencies to develop and implement a rules and consequences policy that facilitates the training and enforcement of adherence by employees, contractors, or others involved in handling PII collected and stored by the federal government, other federal government agencies, or service providers on a federal agency's behalf.

[37] From Federal Register Vol. 71, No. 93, Executive Order 13402 [Internet]. Washington: US Government Printing Office [cited 2011 Oct 2]. Available from: edocket.access.gpo.gov/2006/pdf/06-4552.pdf. *"It is the policy of the United States to use Federal resources effectively to deter, prevent, detect, investigate, proceed against, and prosecute unlawful use by persons of the identifying information of other persons."*

[38] *Cryptographic Module Validation Program (CMVP).* Available from: http://csrc.nist.gov/groups/STM/cmvp/index.html.

EPIC FAIL

Data Security Breaches

On May 7, 2007, the Congressional Research Services (CRS) reported on personal data security breaches to Congress through a report title "Data Security Breaches: Context and Incident Summaries." The breaches were not only due to illegal activity such as hacking or unauthorized employee accesses, but also due to poor security and privacy practices such as lost laptops and posting of personal data to public websites. Highlights of the report [20] that covered business, education, financial, government, and healthcare industries included:

Business

- March 2007—Hacker broke into the website of Johnny's Selected Seeds (Winslow, ME) and stole credit card information in which 20 were used fraudulently.
- February 2007—TJ Maxx computer systems were hacked which resulted in drivers' license numbers, names, and addresses being compromised.

Education

- April 2007—Ohio State University's firewall was bypassed by hackers using foreign Internet in which the names, Social Security numbers, employee identification numbers, and birthdates of current and former staff members was stolen.
- April 2007—University of California, San Francisco's campus server was compromised over a two-year period in which the names, Social Security numbers, and bank accounts for students, faculty, and staff were allegedly affected.

Financial

- December 2006—TD Ameritrade's computers were hacked by criminals using stolen customer accounts requiring them to cover approximately $4 million in fraudulent transactions.
- December 2005—Scottrade Inc. was hacked through the internet in which the customers' names, birth dates, driver's license numbers, phone numbers, bank names, bank routing information, bank account numbers, and Scottrade account numbers were allegedly stolen.

Government

- February 2007—Personal information (names and Social Security numbers) were inadvertently posted to Connecticut State Administrative Services Department's website.
- November 2006—Bowling Green Ohio Police Department inadvertent published personal data (names, Social Security numbers, and phone numbers) to website.

Healthcare

- March 2007—Westerly Hospital in Westerly, RI, allegedly posted patients' confidential information (name, Social Security number, and insurance information) posted on public website.
- Ohio Board of Nursing posted the names and Social Security numbers of nurses to their website twice in one month.

SECURITY AND PRIVACY ISSUES

Overcoming security and privacy issues in public cloud computing requires a federal agency to gain a better understanding of their risks and the necessary security and privacy requirements that need to exist. Using situational analysis techniques such as SWOT[39] (Strengths, Weaknesses, Opportunities, and Threats), a federal agency can analyze the different public cloud service offerings from various CSPs. The analysis can be used to determine if privacy and security-related issues, identified in Table 4.6, believed to have long-term significance for cloud computing [5] exist. In addition, any applicable service agreements (or a separate contract)[40] used can be updated to ensure the CSP satisfies the federal agency's security and privacy requirements.

Table 4.6 Key Security and Privacy Issues and CSP Actions [5]

Issues	CSP Actions
Governance	Align federal agency practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud computing environment.
Compliance	Understand the various types of federal laws and regulations that may impose security and privacy obligations.
Trust	Allow the federal agency visibility into the security and privacy controls and processes employed.
Architecture	Provide the federal agency with technical details into the technologies used to provision the cloud services.
Identity and Access Management	Review in-place safeguards against the federal agency's requirements to ensure it provides adequate security for authentication and authorization, and other identity and access management functions.
Software Isolation	Understand the federal agency's requirements and potential risk associated with using the cloud service virtualization and other logical isolation techniques.
Data Protection	Understand the federal agency's data management requirements to include access control and protection at-rest or in-transit, and deposition.
Availability	Understand the federal agency's availability, data backup and recovery, and disaster recovery requirements.
Incident Response	Align with the federal agency's incident response procedures.

[39] The European Network Information Security Agency (ENISA) *Security & Resilience in Government Clouds* provides an example of using SWOT as a tool as an initial analyzes of different cloud models. Available from: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds.

[40] The Federal CIO Council and Chief Acquisition Officers Council in coordination with the Federal Cloud Complinace Committee to developed Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service, which discusses "Privacy" in contracts (pp. 16–23).

SUMMARY

Public cloud computing presents many opportunities for the federal government to reduce costs and improve operational efficiency. But it requires clear understanding of the security and privacy requirements and examining the risks of the types of information that will be placed in the cloud and requiring an appropriate level of assurance through the application of security service and privacy controls. Although cloud computing is evolving, the application of appropriate frameworks such as the FEA-SPP and tools such as PIAs can assist in predicting the implications and consequences of collecting and storing privacy in a public cloud service.

References

[1] Kundra V. Federal cloud computing strategy. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011.

[2] Federal Chief Information Officers Council, Privacy Committee, Web 2.0/Cloud Computing Subcommittee. Privacy recommendations for the use of cloud computing by federal departments and agencies. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.

[3] Federal Chief Information Officers Council. Federal enterprise architecture security and privacy profile (FEA-SPP), version 3.0. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011.

[4] Mell P, Grance T. NIST Special Publication (SP) 800–145, the NIST definition of cloud computing. Maryland: National Institute of Standards and Technology; 2011.

[5] Jansen W, Grance T. NIST Special Publication (SP) 800–144, guidelines on security and privacy in public cloud computing. Maryland: National Institute of Standards and Technology; 2011.

[6] The Smart Grid Interoperability Panel (SGIP), Cyber Security Working Group. Interagency Report (IR) 7628, guidelines for smart grid security. Maryland: National Institute of Standards and Technology; 2010.

[7] Records, computers and the rights of citizens [Internet]. Washington: US Department of Health & Human Services [cited September 28 2011]. <http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.

[8] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Internet]. Paris: Organisation for Economic Co-operation and Development; [cited September 28 2011]. <http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

[9] Johnson IIIC. Office of Management and Budget (OMB) memorandum 07–16, Safeguarding against and responding to the breach of personally identifiable information. Washington, DC: Executive Office of the President, Office of Management and Budget; 2007.

[10] Overview of the Privacy Act of 1974, 2010 Edition [Internet]. Washington: US Department of Justice [cited September 28 2011]. <http://www.justice.gov/opcl/1974privacyactoverview.htm>.

[11] Privacy Act of 1974 [Internet]. Washington: US Government Printing Office [cited October 10 2011]. <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title5/html/USCODE-2011-title5-partI-chap5-subchapII-sec552a.htm>.

[12] Privacy act issuances [Internet]. Washington: US Government Printing Office [cited October 14 2011]. <http://www.gpoaccess.gov/privacyact/index.html>.

[13] Federal Chief Information Officers Council, Privacy Committee, Web 2.0/Cloud Computing Subcommittee. Privacy recommendations for the use of cloud computing by federal departments and agencies. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.

[14] McCallister E, Grance T, Scarfone K. NIST Special Publication (SP) 800–122, Guide to protecting the confidentiality of Personally Identifiable Information (PII). Maryland: National Institute of Standards and Technology; 2010.

[15] Evans D, Bond P, Bement A. Federal Information Processing Standards (FIPS) 199 Standards for security categorization of federal information and information systems. Maryland: National Institute of Standards and Technology; 2004.

[16] Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800–53 revision 4 (initial public draft), Security and privacy controls for federal information system and organizations. Maryland: National Institute of Standards and Technology; 2012.

[17] Federal Chief Information Officers Council. Federal enterprise architecture security and privacy profile (FEA-SPP), version 3.0. Washington, DC: Office of Management and Budget; 2011.

[18] Federal Privacy Recommendations for the use of cloud computing by federal departments and agencies. Chief Information Officers Council, Privacy Committee, Web 2.0/Cloud Computing Subcommittee. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.

[19] Wood D. Personal information: data breaches are frequent, but evidence resulting identity theft is limited; however, the full extent is unknown. Washington: US Government Accountability Office; 2007.

[20] Tehan R. Data security breaches: context and incident summaries. Washington, DC: Congressional Research Service (CRS); 2007.

[21] Federal CIO Council and Chief Acquisition Officers Council. Creating Effective Cloud Computing Contracts for the Federal Government. Washington, DC: Executive Office of the President, Office of Management and Budget; 2012.

CHAPTER

Applying the NIST Risk Management Framework

5

INFORMATION IN THIS CHAPTER:

- Introduction to FISMA
- Risk Management Framework Overview
- NIST RMF Process

INTRODUCTION TO FISMA

The Federal Information Security Management Act (FISMA) was signed into law on December 17, 2002 as part of the E-Government Act of 2002 (Public Law 107-347). FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000,[1] which expired in November 2002 [1]. FISMA is divided into multiple sections, each of which will be briefly described in this section.

Purpose

FISMA was built upon several existing federal laws designed to ensure the security of federal information and information systems. These federal laws include the Computer Security Act of 1987 (Public Law 100-35),[2] Paperwork Reduction Act of 1995

[1] GISRA directed federal agencies to conduct annual IT security reviews and Inspectors General (IGs) to perform annual independent evaluations of agency programs and systems and report their results to OMB. Available from: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/2002gisra_report.pdf.

[2] From 100th Congress. Public Law 100-235, Computer Security Act of 1987 (40 U.S.C. 759 note). Washington: US Congress; 1987. *"To provide for a computer standards program within the National Bureau of Standards to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes."*

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00005-8

(Public Law 104-13),[3] and Information Technology Management Reform Act of 1996 (i.e., Clinger-Cohen Act, Public Law 104-106, Division E).[4] The purpose of FISMA, as outlined in Section 3541,[5] is covered in six major objectives. In this chapter, the focus will be on 1–4:

1. Establishment of a framework for ensuring the effectiveness of security controls;
2. Development of mechanisms for effective government-wide management and oversight of security-related risks;
3. Development and maintenance of a minimum set of required security controls;
4. Improvement of oversight of information security programs;
5. Utilization of commercially developed information security products for protecting critical information infrastructures; and
6. Selection of commercially developed information security solutions should be left to individual federal agencies.

Role and Responsibilities

The assignment of roles and responsibilities for information security within the federal government was clarified or reiterated within FISMA to cover *policy*, *procurement*, *standards*, and *incident response*. Although FISMA was the last major legislative framework, over the years the foundation has been built upon by a series of Executive Orders, directives, policies, regulations, standards and guidelines. Within FISMA, several specific roles were identified:

- Director of the Office of Management and Budget (OMB).
- National Institute of Standards and Technology (NIST).
- Federal Agencies:
  - Head of Agency or equivalent.
  - Chief Information Officer (CIO).
  - Senior Agency Information Security Officer (SAISO).

[3] From 104th Congress. Paperwork Reduction Act of 1995. Washington: US Congress; 1995. In part it ensured *"the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to the privacy and confidentiality, including section 552a of title 5, security of information, including the Computer Security Act of 1987 (Public Law 100-235); and access to information, including section 552 of title 5."*

[4] Public Law 104-106, Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act) directed the National Institute of Standards and Technology (NIST) to develop standards, guidelines, and associated methods and techniques for federal computer systems. The standards and guidelines issued by NIST, known as Federal Information Processing Standards (FIPS), are used government-wide and developed when there are compelling federal government requirements and there are no existing voluntary standards to address the federal requirements for the interoperability of different systems, the portability of data and software, and computer security.

[5] Section 3541 defined the purpose of the Subchapter III—Information Security.

- Secretary of Defense (SecDef).
- Director of the Central Intelligence Agency (CIA).

In this section, each role will be discussed as it relates to the responsibilities described in FISMA.

Director of OMB

OMB has as one of its key roles[6] the responsibility to implement and enforce government-wide policies. Through FISMA, the Director of OMB was given the authority for overseeing the federal agency implementation and enforcement of security policies and practices. The authorities included:

- Developing and overseeing the implementation of policies, principles, standards, and guidelines on information security (including ensuring timely adoption and compliance by federal agencies);
- Requiring federal agencies to identify and provide for the information security protection for federal information systems and information;
- Coordinating and developing standards and guidelines;
- Overseeing federal agency compliance with FISMA requirements;
- Reviewing (approving/disapproving), at least annually, federal agency information security programs;
- Coordinating information security policies and procedures with related information resources management policies and procedures;
- Overseeing the operation of the federal information security incident center;[7] and
- Reporting annually to Congress on compliance by federal agencies with FISMA requirements (no later than March 1).[8]

These authorities were limited with respect to national security systems (NSSs),[9] except as they relate to budgetary actions and annual reporting to Congress. In this

[6] For additional information on the function of the Office of Management and Budget (OMB), see http://www.whitehouse.gov/omb/organization_mission.

[7] The Federal Computer Incident Response Capability (FedCIRC) resides within the Department of Homeland Security (DHS), National Cyber Security Division (NCSD), Information Analysis and Infrastructure Protection (IA&IP) Directorate. For more information on the IA&IP, see http://www.dhs.gov/xlibrary/assets/CII_Act.pdf.

[8] The annual FISMA report includes: summary of findings of annual independent evaluations (e.g., Office of Inspector General Audits), assessment of adoption and compliance with the NIST standards and guidelines, significant deficiencies in federal agency information security practices, any planned remediation actions to address deficiencies, and summary of a report developed by the NIST.

[9] From E-Government Act of 2002 [Internet]. Washington: US Government Printing Office [cited 2011 Dec 5]. Available from: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm. *Any information system whose function, operations, or use involves intelligence activities, involves cryptographic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapons system, is critical to the fulfillment of military or intelligence missions (excluding any system that is used for administrative and business applications), or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.*

chapter, only those aspects of NSSs related to the NIST Risk Management Framework (RMF) will be discussed.[10]

NIST

NIST, under FISMA, was assigned the responsibility to develop standards, guidelines, and associated methods and techniques for federal agencies. These standards and guidelines include the minimum requirements for providing adequate information security for federal information systems (excluding national security systems):

- Standards to be used for categorizing information and information systems based on objectives of providing an adequate level of information security (*Federal Information Processing Standard (FIPS) PUB 199, Standards for Security Categorization of Federal Information and Information Systems*);
- Guidelines recommending the types of information and information systems (*NIST Special Publication (SP) 800-60 Revision 1, Volume I and II: Guide for Mapping Types of Information and Information System to Security Categories*); and
- Minimum information security requirements (*Federal Information Processing Standard (FIPS) PUB 200, Minimum Security Requirements for Federal Information and Information Systems and NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations*).

NIST was also given the responsibility for developing guidelines for the detection and handling of information security incidents (*NIST Special Publication (SP) 800-61 Revision 2, Computer Security Incident Handling Guide*), and guidelines for identifying an information system as a national security system (*NIST Special Publication (SP) 800-59, Guideline for Identifying an Information System as a National Security System*).[11]

Federal Agencies

Federal agencies are required to comply with the provisions defined in FISMA. As part of their obligation, they must ensure for the protection of federal information

[10] From NIST Special Publication (SP) 800-53, Revision 4 Update Announcement [Internet]. Maryland: National Institute of Standards and Technology [cited 2011 Dec 7]. Available from: http://csrc.nist.gov/groups/SMA/fisma/documents/800-53-Rev4_announcement.pdf. *"As part of the ongoing cyber security partnership among the United States Department of Defense, the Intelligence Community, and the Federal Civil Agencies, five foundational publications are being developed by the partnership's Joint Task Force to create a unified information security framework for the federal government and its contractors."*

[11] From Certification & Accreditation Transformation [Internet]. Maryland: National Institute of Standards and Technology [cited 2011 Dec 27]. Available from: http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=3005. *DoDI 8510.01 aligns with the risk management processes included in NIST SP 800-37 ("Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach") and describes the DoD risk management process, the DoD Information Assurance Risk Management Framework (DIARMF).*

and information systems commensurate with the risk and magnitude of harm resulting from *unauthorized access*, *use*, *disclosure*, *disruption*, *modification*, or *destruction* [2]. This includes complying with information security standards[12] for non-NSSs and standards and guidelines[13] for NSSs. Federal agencies must also ensure information security is an integrated part of their strategic planning and operational planning processes so there is alignment of goals and objectives.

Head of Agency or Equivalent

The Head of the Agency (or the highest-level senior official), in an effort to establish commitment and accountability for information security, was given the responsibility for ensuring senior agency officials (e.g., *authorizing officials*) provide for the protection of federal information and information systems for which they have budgetary oversight, or which support the mission and/or business operations [3]. Protections include:

- Conducting risk assessments;
- Categorizing information and information systems;
- Implementing security policies and procedures; and
- Periodically testing and evaluating security controls and techniques.

The Head of the Agency must ensure security policies, procedures, and practices are adequate. To support this requirement, the Head of the Agency is required to designate a Federal Agency CIO with the authority for the compliance of FISMA. The Federal Agency CIO, in turn, designates his or her IT security responsibilities to a Senior Agency Information Security Officer (SAISO),[14] who is both qualified and trained in information security. These IT security responsibilities include:

- Developing and maintaining an information security program;
- Developing and maintaining information security policies, procedures, and controls;
- Training and overseeing personnel with significant information security responsibilities; and
- Assisting authorizing officials.

[12] From Evans, D., Bond, P., Bement, A. Federal Information Processing Standard (FIPS) PUB 199, Standards for Security Categorization of Federal Information and Information Systems. Maryland: National Institute of Standards and Technology; 2004. *"Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347)."*

[13] From the Committee on National Security Systems (CNSS) [Internet]. Maryland: CNSS [cited 2011 Dec 8]. Available from: http://www.cnss.gov/history.html. *"The CNSS (formerly named the National Security Telecommunications and Information Systems Security Committee (NSTISSC)) was established by National Security Directive (NSD)-42, National Policy for the Security of National Security Telecommunications and Information Systems."*

[14] In most federal agencies the title for this role is the Chief Information Security Officer (CISO).

Federal Agency Information Security Program

Federal agencies are also required to establish an agency-wide information security program. The program developed by the federal agency must address the following requirements:

- Security awareness training;
- Risk assessments;
- Policies and procedures;
- Integration of security into the system development lifecycle;
- Compliance programs that include security planning, testing, and remediation;
- Incident response capability; and
- Continuity of operations planning.

Federal Agency Independent Evaluations and Reporting

On an annual basis, federal agencies are required by law to conduct an independent evaluation of their information security program to ensure its effectiveness. The independent evaluations involve the testing of the effectiveness of the organization's policies, procedures, and practices, and an assessment compliance with FISMA, including any supporting federal policies, procedures, standards, and guidelines. The results of the independent evaluations are sent through the Head of the Agency to the Director of OMB. The Director of OMB includes information from all independent evaluations across the federal government and develops a comprehensive summary in a government-wide report that is submitted to Congress.[15]

TIP

To support federal agencies in evaluating their programs, NIST developed the Program Review for Information Security Management Assistance (PRISMA).[16] The PRISMA methodology uses "a standardized approach to review and measure the information security posture of an information security program" [4]. The PRISMA process includes 11 steps that cover both *preparation* and *execution*.

Preparation Steps:

- Review initiation.
- Review scope definition.
- Planning.
- Kickoff meeting.

Execution Steps:

- Review execution.
- Review documentation.

[15] OMB reports to Congress no later than March 1st of each year.

[16] *Program Review for Information Security Management Assistance (PRISMA)*. Available from: http://csrc.nist.gov/groups/SMA/prisma/index.html.

- Interviews.
- Environmental influences and constraints.
- Team negotiations.
- Analysis, report generation, and review.

RISK MANAGEMENT FRAMEWORK OVERVIEW

The NIST RMF[17] is a flexible, risk-based approach that is driven by the organization's information security program, and supports the management of risk[18] by facilitating the sharing[19] of information. The NIST RMF objectives [4] include:

- Building information security capabilities into federal information systems;
- Maintaining awareness of the security state of information systems through ongoing continuous monitoring; and
- Providing essential information to key stakeholders to facilitate decisions regarding the acceptance of risk.

Risk management is an essential element of the NIST RMF, which requires linking risks to an organization-wide information security program. This enables the organization to have a broader view of risks, including those across all information systems within the enterprise. Since the NIST RMF is a more technical approach, organizations will need to ensure risk-based decisions are considered from a strategic viewpoint where the impact to the organization's goals and objectives is more visible.

For the NIST RMF to be effective, the organization needs to identify and communicate program-level security requirements that all information systems within the enterprise should meet. This also limits the duplication of risk management activities

[17] The NIST RMF was developed by the Joint Task Force Transformation Initiative (JTFTI) Working Group, a partnership with stakeholders from the US Department of Defense (DoD), Intelligence Community (IC), and NIST, as a common framework for government-wide risk management.

[18] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes."*

[19] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Reciprocity is the mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information."*

where common capabilities can be integrated or even shared by each information system within the overall organization-wide information security program. In this section, we will briefly discuss the role of the risk management when applying the NIST RMF and how closely aligning the system development life cycle (SDLC) processes enables security-related information produced during the SDLC to be reused to support the risk management process.

The Role of Risk Management

The effective application of the NIST RMF requires the integration of risk management[20] activities at different levels within an organization. As illustrated in Figure 5.1, the risk management process begins at the organizational level (*Tier 1*) where the governance structure and risk management strategy are developed.

The risk management strategy[21] supports the organization's strategic goals and objectives. To link the risk management strategy with the mission and business processes (*Tier 2*), risk management should be addressed as a part of the enterprise architecture.[22] Finally, at the information system level (*Tier 3*), the appropriate safeguards and countermeasures are applied to the information and information system through the selection, implementation, and assessment of security controls that have traceability to the security requirements established by the organization and allocated within the information security architecture. This alignment between the NIST RMF and the SDLC is critical to ensure there is an early integration of security with the appropriate inputs from stakeholders across the organization.

The NIST RMF and the System Development Life Cycle

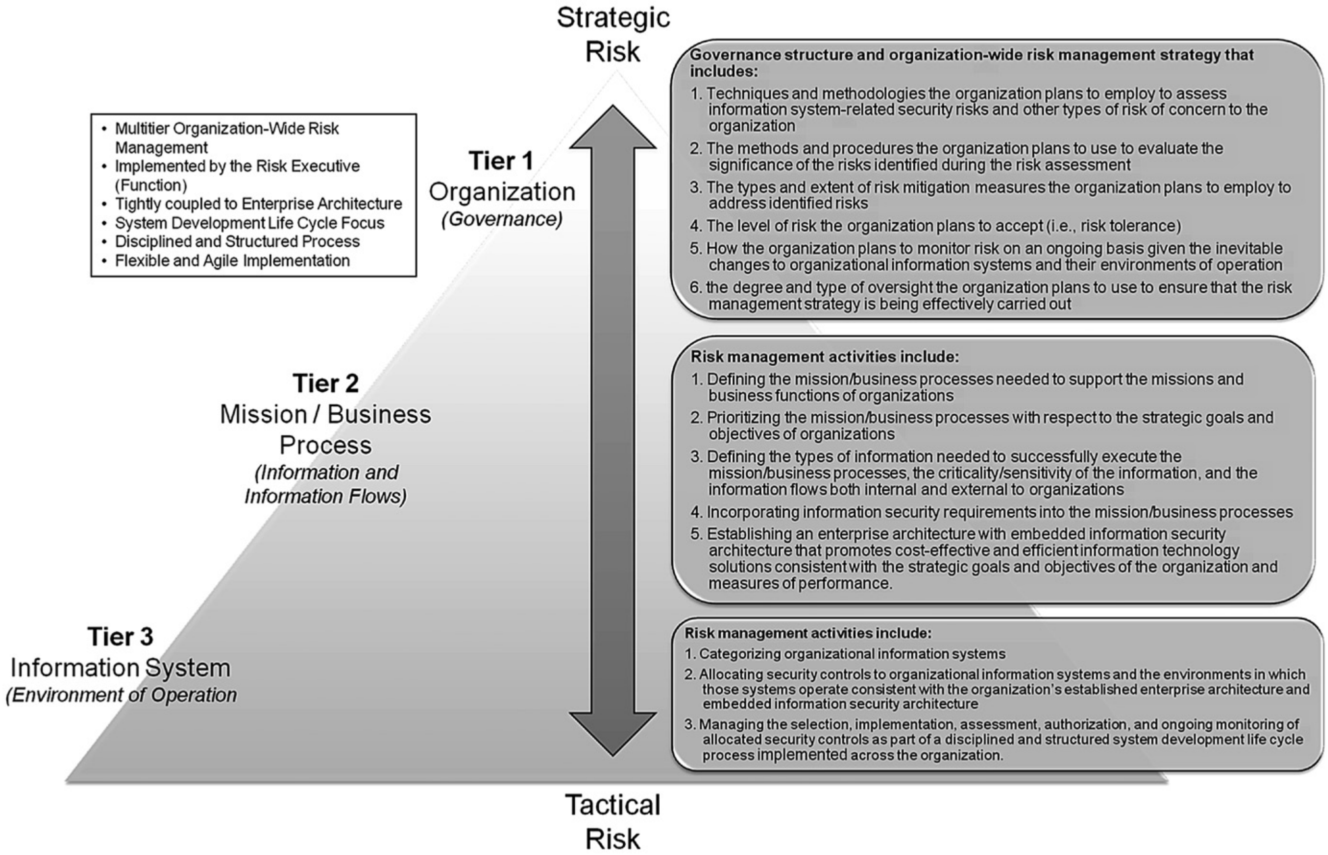
As previously discussed, the alignment of activities included in the NIST RMF with a traditional SDLC[23] ensures risk management becomes an integrated part of the

[20] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time."*

[21] The Risk Management Strategy will be discussed in detail in Chapter 6, Risk Management.

[22] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. The security categorization process is conducted as an organization-wide activity taking into consideration the enterprise architecture and the information security architecture to ensure that individual information systems are categorized based on the mission and business objectives of the organization.

[23] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"There are typically five phases in a generic system development life cycle including: (i) initiation; (ii) development/acquisition; (iii) implementation; (iv) operation/maintenance; and (v) disposal."*



- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation

Governance structure and organization-wide risk management strategy that includes:

1. Techniques and methodologies the organization plans to employ to assess information system-related security risks and other types of risk of concern to the organization
2. The methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment
3. The types and extent of risk mitigation measures the organization plans to employ to address identified risks
4. The level of risk the organization plans to accept (i.e., risk tolerance)
5. How the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation
6. the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out

Risk management activities include:

1. Defining the mission/business processes needed to support the missions and business functions of organizations
2. Prioritizing the mission/business processes with respect to the strategic goals and objectives of organizations
3. Defining the types of information needed to successfully execute the mission/business processes, the criticality/sensitivity of the information, and the information flows both internal and external to organizations
4. Incorporating information security requirements into the mission/business processes
5. Establishing an enterprise architecture with embedded information security architecture that promotes cost-effective and efficient information technology solutions consistent with the strategic goals and objectives of the organization and measures of performance.

Risk management activities include:

1. Categorizing organizational information systems
2. Allocating security controls to organizational information systems and the environments in which those systems operate consistent with the organization's established enterprise architecture and embedded information security architecture
3. Managing the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls as part of a disciplined and structured system development life cycle process implemented across the organization.

FIGURE 5.1 Tiered Risk Management Approach

information system life cycle. At each phase of the SDLC, as illustrated in Figure 5.2, specific security considerations are integrated, starting at the initiation phase where requirements definition begins.

Security requirements[24] addressed later within the SDLC instead of including them in the original system design could unnecessarily increase costs and delay the authorization process. By defining NIST RMF activities within the context of the system development process, weaknesses and deficiencies identified early in the SDLC could improve the effectiveness of security testing performed later in the NIST RMF (e.g., assessing and monitoring security controls). Since information systems typically exist at some phase of the SDLC and will continue to evolve throughout their life cycle, integrating the NIST RMF into the life cycle process enables risks to be mitigated or eliminated through information security and risk management–related activities. For example, the security-related information produced through development security testing may be reused later in SDLC (e.g., implementation/assessment or the operation/maintenance phases).

NIST RMF PROCESS

The NIST RMF is a task-oriented process that is driven by the risk management activities applied at all levels of the organization. The tasks addressed within the NIST RMF include different risk-related activities that support the organization's risk management strategy. Since Chapter 6 will cover enterprise-wide risk management in more detail, this chapter will limit the focus of risk management as it relates to the information system (*Tier 3*), as shown in Figure 5.1. The risk management activities included in Figure 5.3 involve applying the steps included within the NIST RMF as a part of a security life cycle approach. The steps performed within the NIST RMF include:

- categorize the information and information system,
- select the security control baseline,
- implement the selected security controls,
- assess the security controls,
- authorize information system operation, and
- monitor the security controls.

[24] From Kissel, R., Stine K., Scholl, M., Rossman, H., Fahlsing, J., Gulick. NIST Special Publication (SP) 800-64 Revision 2, Security Considerations in the System Development Lifecycle. Maryland: National Institute of Standards and Technology; 2008. *"Security requirements are a subset of the overall functional and nonfunctional (e.g. quality, assurance) requirements levied on an information system and are incorporated into the system development life cycle simultaneously with the functional and nonfunctional requirements."*

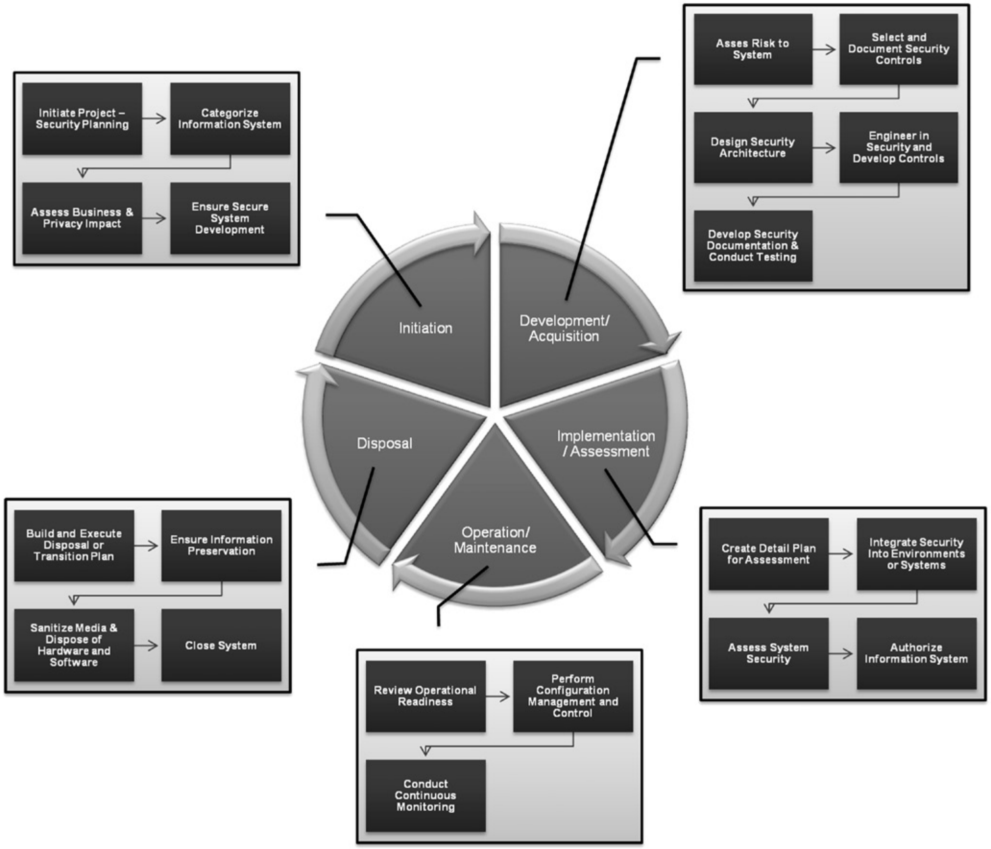
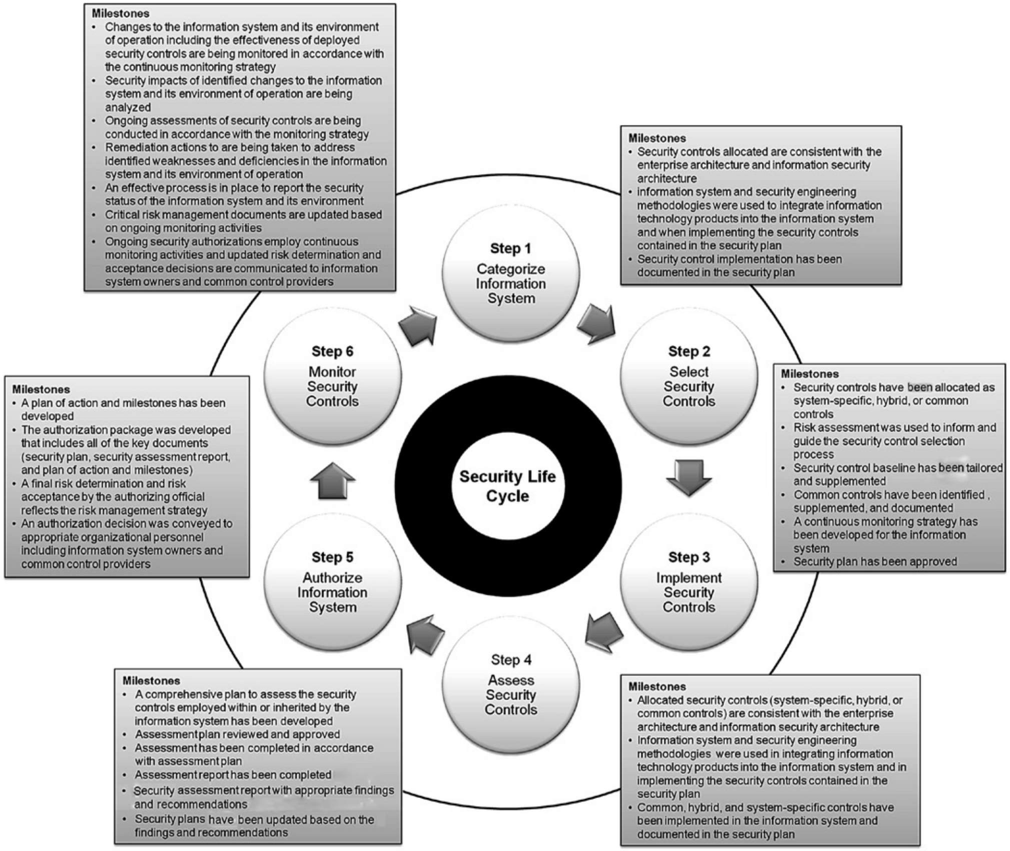

Initiation
Development/ Acquisition
Implementation / Assessment
Operation/ Maintenance
Disposal
Initiate Project – Security Planning
Categorize Information System
Assess Business & Privacy Impact
Ensure Secure System Development
Asses Risk to System
Select and Document Security Controls
Design Security Architecture
Engineer in Security and Develop Controls
Develop Security Documentation & Conduct Testing
Create Detail Plan for Assessment
Integrate Security Into Environments or Systems
Assess System Security
Authorize Information System
Review Operational Readiness
Perform Configuration Management and Control
Conduct Continuous Monitoring
Build and Execute Disposal or Transition Plan
Ensure Information Preservation
Sanitize Media & Dispose of Hardware and Software
Close System

FIGURE 5.2 Security Consideration in the System Development Lifecycle (SDLC)


Security Life Cycle
Step 1
Categorize Information System
Step 2
Select Security Controls
Step 3
Implement Security Controls
Step 4
Assess Security Controls
Step 5
Authorize Information System
Step 6
Monitor Security Controls

Milestones
- Security controls allocated are consistent with the enterprise architecture and information security architecture
- information system and security engineering methodologies were used to integrate information technology products into the information system and when implementing the security controls contained in the security plan
- Security control implementation has been documented in the security plan

Milestones
- Security controls have been allocated as system-specific, hybrid, or common controls
- Risk assessment was used to inform and guide the security control selection process
- Security control baseline has been tailored and supplemented
- Common controls have been identified , supplemented, and documented
- A continuous monitoring strategy has been developed for the information system
- Security plan has been approved

Milestones
- Allocated security controls (system-specific, hybrid, or common controls) are consistent with the enterprise architecture and information security architecture
- Information system and security engineering methodologies were used in integrating information technology products into the information system and in implementing the security controls contained in the security plan
- Common, hybrid, and system-specific controls have been implemented in the information system and documented in the security plan

Milestones
- A comprehensive plan to assess the security controls employed within or inherited by the information system has been developed
- Assessment plan reviewed and approved
- Assessment has been completed in accordance with assessment plan
- Assessment report has been completed
- Security assessment report with appropriate findings and recommendations
- Security plans have been updated based on the findings and recommendations

Milestones
- A plan of action and milestones has been developed
- The authorization package was developed that includes all of the key documents (security plan, security assessment report, and plan of action and milestones)
- A final risk determination and risk acceptance by the authorizing official reflects the risk management strategy
- An authorization decision was conveyed to appropriate organizational personnel including information system owners and common control providers

Milestones
- Changes to the information system and its environment of operation including the effectiveness of deployed security controls are being monitored in accordance with the continuous monitoring strategy
- Security impacts of identified changes to the information system and its environment of operation are being analyzed
- Ongoing assessments of security controls are being conducted in accordance with the monitoring strategy
- Remediation actions to are being taken to address identified weaknesses and deficiencies in the information system and its environment of operation
- An effective process is in place to report the security status of the information system and its environment
- Critical risk management documents are updated based on ongoing monitoring activities
- Ongoing security authorizations employ continuous monitoring activities and updated risk determination and acceptance decisions are communicated to information system owners and common control providers

FIGURE 5.3 Risk Management Framework

Information System Categorization

The *categorization* of the information system is the first step in the NIST RMF (*Step 1*), and one of the most essential activities[25] required for the selection of a baseline set of security controls (and privacy controls, where applicable). As discussed earlier in the chapter, FISMA tasked NIST with the responsibility to develop standards and guidelines. The standards included procedures for categorizing information and information systems, and the guidelines for categorizing the different types[26] of federal information that will be processed, stored, or transmitted within the information system. The first step in the NIST RMF (*Step 1*), as shown in Table 5.1, includes three major tasks. In this section, the discussion will primarily focus on the first task (1-1).

The security categorization process is driven by the need for federal agencies (or others operating on behalf of federal agencies) to identify the types of information[27] that will be processed, stored, or transmitted in the information system, a critical requirement for understanding the security objectives (confidentiality,[28] integrity,[29] and availability[30]). In addition, the security categorization process also ensures the

[25] From Evans, D., Bond, P., Bement, A. Federal Information Processing Standard (FIPS) PUB 199, Standards for Security Categorization of Federal Information and Information Systems. Maryland: National Institute of Standards and Technology; 2004. *"Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization."*

[26] From Evans, D., Bond, P., Bement, A. Federal Information Processing Standard (FIPS) PUB 199, Standards for Security Categorization of Federal Information and Information Systems. Maryland: National Institute of Standards and Technology; 2004. *"Information type is a specific category of information (e.g. privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive order, or directive, policy, or regulation."*

[27] From Evans, D., Bond, P., Bement, A. Federal Information Processing Standard (FIPS) PUB 199, Standards for Security Categorization of Federal Information and Information Systems. Maryland: National Institute of Standards and Technology; 2004. *FIPS 199 applies to all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status and all federal information systems other than those information systems designated as national security systems.*

[28] From E-Government Act of 2002 [Internet]. Washington: US Government Printing Office [cited 2011 Dec 9]. Available from: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm. *"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."*

[29] From E-Government Act of 2002 [Internet]. Washington: US Government Printing Office [cited 2011 Dec 9]. Available from: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347. htm. *"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."*

[30] From E-Government Act of 2002 [Internet]. Washington: US Government Printing Office; [cited 2011 Dec 9]. Available from: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107 publ347.htm. *"Ensuring timely and reliable access to and use of information."*

Table 5.1 NIST RMF Step 1 Activities [3]

Task	Name	Activities	References
1-1	Security categorization	• Categorize the information system • Document the results of the security categorization in the security plan	• FIPS 199 • NIST SP 800-30 • NIST SP 800-39 • NIST SP 800-59 • NIST SP 800-60 • CNSS Instruction 1253
1-2	Information system description	• Describe the information system (including the system boundary) • Document the description in the security plan	
1-3	Information system registration	• Register the information system with appropriate organizational program/management offices	

selected security controls implemented provide the adequate security[31] to meet the organization's security objectives. As will be discussed in detail in this chapter, the application of a standardized approach to categorizing information systems enables a common framework to be used across the federal government for the management and oversight of information systems and in reports relating to agency-specific information security to OMB and government-wide information security to Congress.

The application of the security categorization process becomes complex when external information system services[32] are used by federal agencies in processing, transmitting, or storing information collected or maintained on behalf of the federal government. In these instances, a federal agency's reliance upon an external service does not limit its overall responsibility for ensuring the security categorization of the external service being used is consistent with the different types of information that will be used within the service to support its mission or business needs. Without an understanding of the security categorization of the information being used in the external service, the federal agency will not be able to determine the necessary requirements

[31] From Office of Management and Budget (OMB.) Security of Federal Automated Information Resources [Internet]. Washington: Executive Office of the President, Office of Management and Budget [cited 2011 Dec 9]. Available from: http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii. *Adequate security is "security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."*

[32] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"A service for which the organization typically no direct control over the application of required security controls or the assessment of security control effectiveness."*

that must be used by the service provider to ensure the service operates at a security level consistent with the federal agency's minimum assurance requirements.

Relationship Between the NIST RMF and the Federal Enterprise Architecture

The enterprise architecture is a management practice employed to maximize the effectiveness of mission/business process and information resources [5]. As illustrated in Figure 5.4, the enterprise assets identified within the enterprise architecture are mapped to the individual federal agency's mission and business processes through the reference models provided in the Federal Enterprise Architecture (FEA)[33] and the resulting segment architecture.[34] The application of the mapping ensures the information resources are properly aligned with each federal agency's strategic goals and objectives.

The relationship between the federal agency's enterprise architecture[35] and the application of the NIST RMF begins with the initial security categorization. Security categorization provides a vital step in integrating security into the business and information technology management functions and establishes the foundation for information security standardization.[36] The security categorization process is largely dependent upon the knowledge of the information supporting the federal government. By utilizing a framework similar to the one depicted in Figure 5.5, the security categorization process is adopted as an enterprise-level viewpoint for "each type of information as identified from the FEA Performance Reference Model (PRM)[37] and Business Reference Model (BRM)[38] analysis" [6]. This produces a government-wide

[33] From Federal Chief Information Officers Council. Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP), version 3.0. Washington: Office of Management and Budget; 2011. *"The FEA is a business-based framework for government-wide improvement. The goals of the FEA are to locate and reduce or eliminate duplicative investments, discover areas where investments should be made, and identify where departments and agencies can collaborate to improve government operations or services."*

[34] From Federal Chief Information Officers Council. Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP), version 3.0. Washington: Office of Management and Budget; 2011. *"Segment architecture drives decisions for a business case or group of business cases supporting a core mission area or common or shared service."*

[35] From Federal Chief Information Officers Council. Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP), version 3.0. Washington: Office of Management and Budget; 2011. *"A strategic information asset base which defines the mission, the information necessary to perform the mission and the transitional processes for implementing new technologies in response to the changing mission needs."*

[36] Federal Chief Information Officers Council. Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP), Version 3.0. Washington: Office of Management and Budget; 2011.

[37] From Federal Chief Information Officers Council. Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP), version 3.0. Washington: Office of Management and Budget; 2011. *Performance Reference Model (PRM) is information that helps agencies monitor the performance of an investment and/or program.*

[38] From Federal Chief Information Officers Council. Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP), version 3.0. Washington: Office of Management and Budget; 2011. *Business Reference Model (BRM) is information that helps agencies understand what primary business functions are provided to citizens through the definition of business areas, lines of business, and sub-functions.*

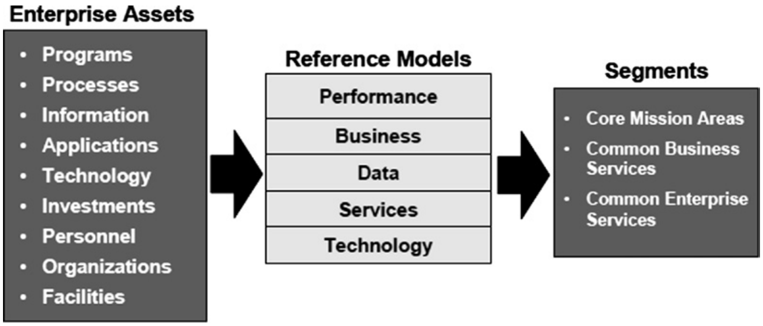


FIGURE 5.4 Enterprise Asset Mapping [19]

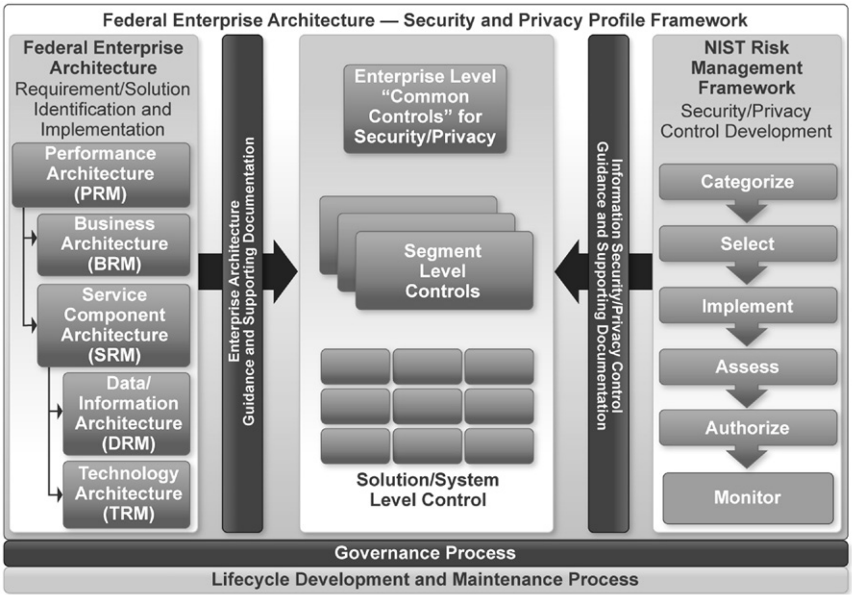

Federal Enterprise Architecture — Security and Privacy Profile Framework
Federal Enterprise Architecture
Requirement/Solution Identification and Implementation
Performance Architecture (PRM)
Business Architecture (BRM)
Service Component Architecture (SRM)
Data/ Information Architecture (DRM)
Technology Architecture (TRM)
Enterprise Architecture Guidance and Supporting Documentation
Enterprise Level "Common Controls" for Security/Privacy
Segment Level Controls
Solution/System Level Control
Information Security/Privacy Control Guidance and Supporting Documentation
NIST Risk Management Framework
Security/Privacy Control Development
Categorize
Select
Implement
Assess
Authorize
Monitor
Governance Process
Lifecycle Development and Maintenance Process

FIGURE 5.5 Federal Enterprise Architecture—Security and Privacy Profile Framework [6]

approach for evaluating the "level of potential impact values assigned to the respective security objectives" [7] (i.e., confidentiality, integrity, and availability) that are used for establishing the information security and privacy requirements in the security control selection step of the NIST RMF (*Step 3*). The results provide for a strong linkage between the mission, the information, and the information systems with a focus on cost-effective application of information security [8].

Shared Responsibility and the Chain of Trust

In general, the application of the NIST RMF requires a shared responsibility and a chain of trust.[39] The relationship between federal agencies and service providers requires operating through terms and conditions defined in a contract, which includes detailed security control requirements, or managed through a service level agreement (SLA).[40] Service providers handling federal information or operating information systems on behalf of the federal government must meet the same security requirements as federal agencies [3]. Therefore, the security categorization of the information can provide a common understanding of the security objectives that drive the selection and compensation of security control requirements that need to be implemented. The security categorization process also ensures service providers have some knowledge of the types of information that will be processed and the potential overall impact to the federal government should certain adverse events occur.

Service providers have a responsibility in maintaining an adequate level of security to protect the information throughout the service life cycle. However, the overall responsibility to ensure that sufficient security exists to meet the information protection requirements falls on the authorizing official.[41] For a chain of trust, operating under a shared responsibility model, to exist between the federal government and service providers, confidence needs to be gained through an understanding of the security controls implemented in the service and its environment. This confidence is achieved by verifiable and credible evidence that the security controls are operating effectively. Trust becomes even more important under complex consumer-provider relationships that are introduced such as multi-vendor situations. By establishing a clear definition of the security objectives, an analysis[42] can be performed to determine

[39] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"A chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization."*

[40] From Jansen, W., Grance, T. NIST Special Publication (SP) 800-144, Guidelines on Security and Privacy in Public Cloud Computing. Maryland: National Institute of Standards and Technology; 2011. *"An SLA represents the understanding between the cloud subscriber and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation available to the cloud subscriber."*

[41] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The authorizing official is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the Nation."*

[42] From Badger, L., Bernstein, D., Bohn, R., de Vaulx, F., Hogan, M., Mao, J., et al. NIST Special Publication (SP) 500-293 (Draft), US Government Cloud Computing Technology Roadmap, Release 1.0. Maryland: National Institute of Standards and Technology; 2011. *"This analysis needs to include considerations from a service model perspective, where different service models imply different degrees of control between cloud providers and cloud consumers."*

which participant, consumer or provider, would be most appropriate to implement the necessary security controls based on the differing degrees of ownership and control over the information system.

Overview of the Security Categorization Process

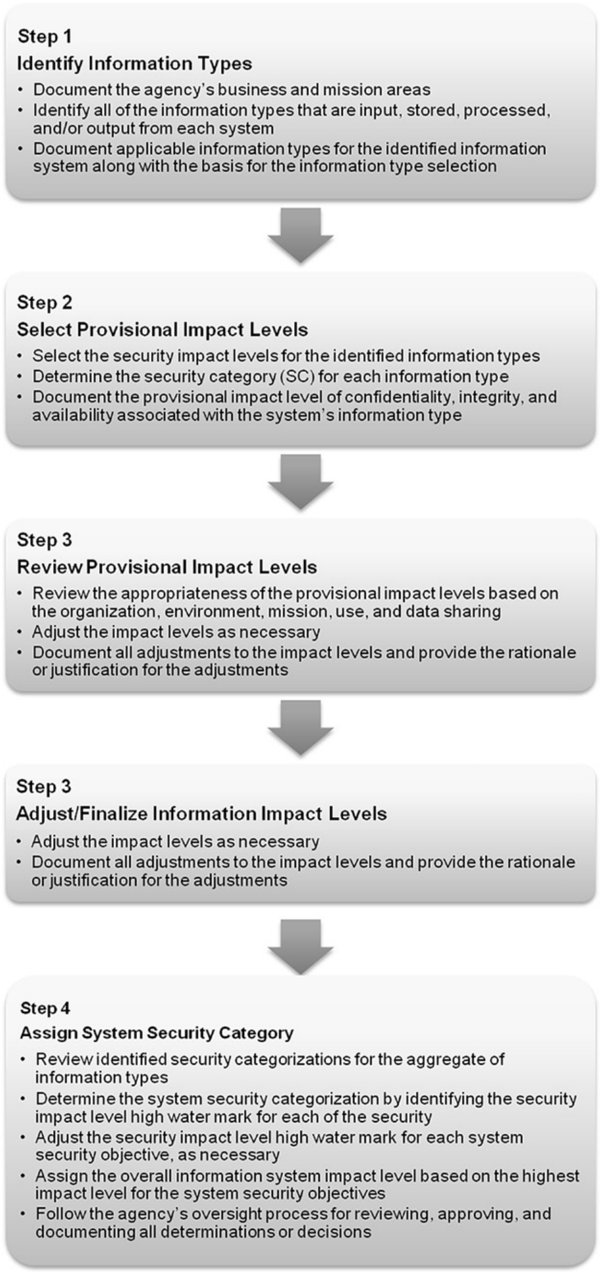
The goal of the security categorization process is to understand, identify, and categorize both the information and information systems used to process, store, or transmit the information, so that an appropriate level of information security can be applied. The level of information security is determined, in part, through an assessment of the potential impact[43] to the information in the event that there was a compromise (e.g., breach of security) which caused a loss in confidentiality, integrity, or availability. The results of this process enable federal agencies to understand and communicate their protection requirements as a consequence (e.g., degradation of primary mission functions or capabilities, financial loss, etc.) to an adverse impact to their mission and business processes. In addition, by managing the risk at the enterprise level, the information security needs can be applied more effectively across the federal government by an aggregation of the sensitivity/criticality of information using a standardized and common language. This ensures information systems supporting multiple federal agency mission areas or supporting federal agencies as a shared business service[44] operate based on the highest level of impact to the federal government.

The security categorization process requires input from across all stakeholders. For this process to be successful the federal agency needs to ensure coordination and collaboration exist among all parties involved (e.g., information owners, information security practitioners, enterprise architects, capital planning, etc.). Since the output of this process will be an input to the remaining steps in the NIST RMF (*Steps 2–6*), oversight is critical to ensure any errors can be validated to prevent or minimize overprotection or potentially increasing organizational risk by underprotecting the information resources.

Before the categorization process can begin, information to support the categorization process needs to be collected, including the specific organizational-specific policies, procedures, and other relevant documentation relating to risk management that would help the organization understand impacts associated with the loss of confidentiality, integrity, and availability. As depicted in Figure 5.6, the categorization process is a multi-step activity that begins with the identification of information types and concludes with the assignment of security categories and impact levels to

[43] From Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick J. NIST Special Publication (SP) 800-60 Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Maryland: National Institute of Standards and Technology; 2008. *"An incorrect information system impact can result in the agency either over protecting the information system thus wasting valuable security resources, or under protecting the information system and placing important operations and assets at risk."*

[44] From Office of Management and Budget (OMB). Federal Information Technology Shared Services Strategy. Washington: Executive Office of the President, Office of Management and Budget; 2012. *"A function that is provided for consumption by multiple organizations within or between Federal Agencies."*



Step 1
Identify Information Types

- Document the agency's business and mission areas
- Identify all of the information types that are input, stored, processed, and/or output from each system
- Document applicable information types for the identified information system along with the basis for the information type selection

Step 2
Select Provisional Impact Levels

- Select the security impact levels for the identified information types
- Determine the security category (SC) for each information type
- Document the provisional impact level of confidentiality, integrity, and availability associated with the system's information type

Step 3
Review Provisional Impact Levels

- Review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing
- Adjust the impact levels as necessary
- Document all adjustments to the impact levels and provide the rationale or justification for the adjustments

Step 3
Adjust/Finalize Information Impact Levels

- Adjust the impact levels as necessary
- Document all adjustments to the impact levels and provide the rationale or justification for the adjustments

Step 4
Assign System Security Category

- Review identified security categorizations for the aggregate of information types
- Determine the system security categorization by identifying the security impact level high water mark for each of the security
- Adjust the security impact level high water mark for each system security objective, as necessary
- Assign the overall information system impact level based on the highest impact level for the system security objectives
- Follow the agency's oversight process for reviewing, approving, and documenting all determinations or decisions

FIGURE 5.6 Security Categorization Process

information and information systems[45] that will be used as the basis for establishing the initial baseline set of security controls.

Identify Information Types

In July 2001, OMB issued *Citizen-Centered E-Government: Developing the Action Plan*,[46] which established an E-Government Task Force to "identify priority actions that achieve strategic improvements in government and set in motion a transformation of government around citizen needs" [9]. The task force published the E-Government Strategy[47] which focused on achieving improvements across multiple business areas of service within the federal government and reforming the efficiency and effectiveness of the federal government's interaction with individual citizens, businesses, other state and local governments, and even internally within the federal government itself. As part of the assessment[48] performed by the task force, a business architecture, shown in Figure 5.7, was created as a framework to "describe how the federal government interfaces with citizens, what functions and lines of business the government performs, and the key business processes used" [9].

As the foundation for the FEA BRM,[49] the FEA Program Management Office (FEAPMO) "leveraged previous Federal architecture efforts, in particular the business architecture designed as a part of the 2001 e-government Task Force's effort, as starting points for designing the government-wide model" [10]. Since its initial release, the business architecture has been through multiple revisions. The BRM version 2.0, depicted in Figure 5.8, reflects four business areas (functions): services for citizens, mode of delivery, support delivery of services, and management of government resources. The BRM is a framework that uses a structured tiered hierarchical representation for describing the common business areas within the federal government.

The federal government's dependence on information technology (IT) to support various mission and business functions requires federal agencies to understand the appropriate security controls that need to be implemented. The security controls are

[45] From US Code, Title 44, Chapter 35: Coordination of Federal Information Policy [Internet]. Washington: US Government Printing Office [cited 2011 Dec 11]. Available from: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm. *"An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."*

[46] Office of Management and Budget (OMB) Memorandum 01-28. Available from: http://www.whitehouse.gov/omb/memoranda_m01-28

[47] *Simplified Delivery of Services to Citizens*. Available from: http://www.cio.gov/documents/egovstrategy.html.

[48] From E-Government Task Force. E-Government Strategy. Washington: Executive Office of the President, Office of Management and Budget; 2002. *The assessment applied the approach of the Federal Chief Information Officers Council, using the enterprise architecture to establish a "roadmap to achieve an agency's mission through optimal performance of its core business processes within an efficient IT environment."*

[49] The Business Reference Model (BRM) version 1.0 was published in July 2002 and version 2.0 was published in June 2003.

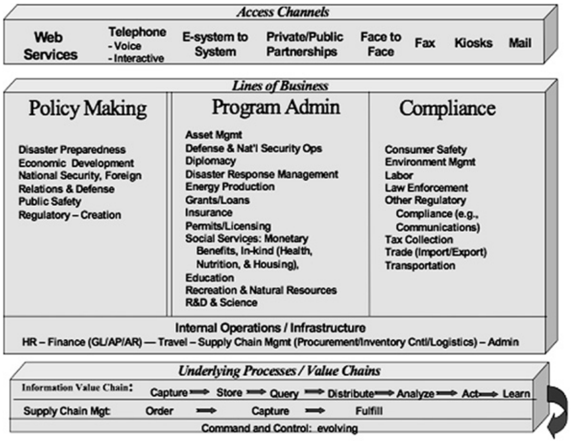


FIGURE 5.7 Business Architecture [9]

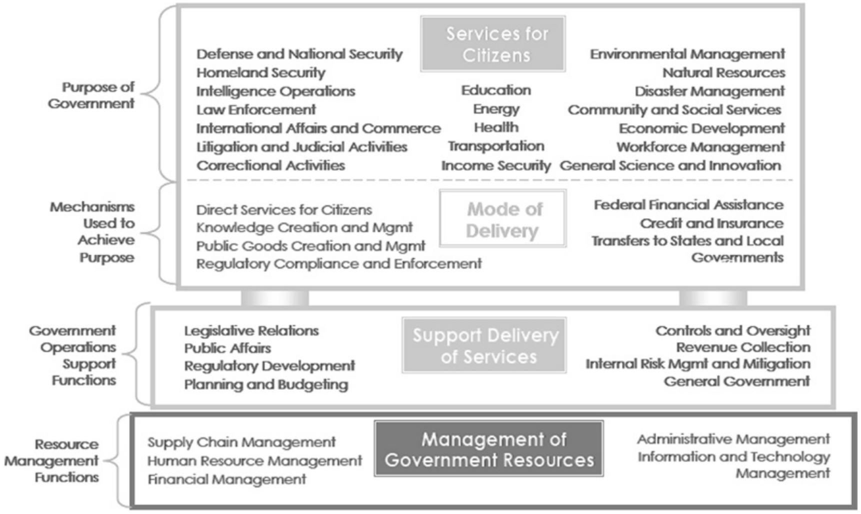

Purpose of Government
Mechanisms Used to Achieve Purpose
Government Operations Support Functions
Resource Management Functions
Services for Citizens
Defense and National Security
Homeland Security
Intelligence Operations
Law Enforcement
International Affairs and Commerce
Litigation and Judicial Activities
Correctional Activities
Education
Energy
Health
Transportation
Income Security
Environmental Management
Natural Resources
Disaster Management
Community and Social Services
Economic Development
Workforce Management
General Science and Innovation
Mode of Delivery
Direct Services for Citizens
Knowledge Creation and Mgmt
Public Goods Creation and Mgmt
Regulatory Compliance and Enforcement
Federal Financial Assistance
Credit and Insurance
Transfers to States and Local Governments
Support Delivery of Services
Legislative Relations
Public Affairs
Regulatory Development
Planning and Budgeting
Controls and Oversight
Revenue Collection
Internal Risk Mgmt and Mitigation
General Government
Management of Government Resources
Supply Chain Management
Human Resource Management
Financial Management
Administrative Management
Information and Technology Management

FIGURE 5.8 Business Reference Model 2.0 [11]

identified through an assessment of potential impacts should there be a breach of security (i.e., a loss of confidentiality) [7]. Therefore, the first step in the security categorization process requires the identification of information types be processed, transmitted, or stored in the information system. Since the BRM is periodically updated[50] to provide a government-wide view of the various business areas and

[50] FEA BRM Version 3.0. Available from: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fea_brmv3_wdefinitions_20120622_final.xlsx

TIP

The types of activities [8] associated with the identification of information types are:

- Document the agency's business and mission areas.
- Identify all of the information types that are input, stored, processed, and/or output from each system.
  - Identify *Mission-based* Information Type categories based on supporting FEA Lines of Business.
  - As applicable, identify *Management and Support* Information Type categories based on supporting FEA Lines of Business.
  - Specify applicable sub-functions for the identified *Mission-based* and *Management and Support* categories.
  - As necessary, identify other required information types.
- Document applicable information types for the identified information system along with the basis for the information type selection.

functions across the federal government, NIST used the BRM as the basis for the taxonomy of information types[51] for federal agencies to reference[52] when mapping the information types used in the information system. The integration of the enterprise architecture developed by the federal agency can provide a useful starting point to ensure the categorization is consistent with the mission and business objectives.

Select Provisional Impact Values for Each Information Type

Once the information types have been identified and documented, the provisional impact levels need to be selected and assigned to the security objectives of each information type. The provisional impact levels[53] are based on the potential impacts included in Table 5.2. From the provisional impact levels, an initial security categorization is characterized using the following format:

Security Category $_{\text{information type}}$ = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}

[51] From Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick, J. NIST Special Publication (SP) 800-60 Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Maryland: National Institute of Standards and Technology; 2008. *NIST Special Publication (SP) 800-60 (Volume I & II) provides guidelines for agencies to use in categorizing information and information systems by "recommending the types of information and information systems to be included in each such category of potential impact."*

[52] There are instances where information used in an information system may not be captured in the BRM, which will require federal agencies to conduct additional research when characterizing the information so that appropriate impact levels can be assigned to the security categories.

[53] The provisional impact for each information type is documented in Volume II of NIST SP 800-60.

Table 5.2 Potential Impact Levels [7]

Potential Impact	Definition
Low	• The potential impact is *low* if the loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals
Moderate	• The potential impact is *moderate* if the loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals • A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries
High	• The potential impact is *high* if the loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals • A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

NOTE

The types of activities [8] associated with the selection of provisional impact levels are:

- Select the security impact levels for the identified information types from the recommended provisional impact levels for each identified information type or from FIPS 199 criteria.
- Determine the security category (SC) for each information type: SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}.
- Document the provisional impact level of confidentiality, integrity, and availability associated with the system's information type.

Adjust the Information Type's Provisioning Impact Value and Security Category

After the provisional impact levels have been selected, adjustments can be applied (as required) to the information types using information about the information system's environment such as the federal agency's mission, how the information will be used, and interfaces with other systems outside of the authorization boundary[54] (or information system boundary). Other considerations might also include special factors specific to each security category as it applies to the organization or individuals[55] should a specific breach of security occur. When all of the adjustments to the provisional impact levels have been made for an information type, the highest impact value from each of the selected security objectives becomes the overall security categorization for the information type. As an example, the security categorization for the following information type would be *Moderate* (see Table 5.3).

Security Category $_{\text{information type}}$ = {(**confidentiality**, *moderate*), (**integrity**, *moderate*), (**availability**, *low*)}

TIP

The types of activities [8] associated with the review of the provisional impact levels and the adjustment and finalization of the information impact levels include:

- Reviewing the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing.
- Adjusting the impact levels (as necessary) based on confidentiality, integrity, and availability factors, situational and operational drivers (timing, lifecycle, etc.), and legal or statutory reasons.
- Documenting all adjustments to the impact levels and providing the rationale or justification for the adjustments.

Security Category $_{\text{information type}}$ = {(**confidentiality**, *moderate*), (**integrity**, *moderate*), (**availability**, *low*)}

[54] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected."*

[55] From Evans, D., Bond, P., Bement, A. Federal Information Processing Standard (FIPS) PUB 199, Standards for Security Categorization of Federal Information and Information Systems. Maryland: National Institute of Standards and Technology; 2004. *"Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law."*

Security Category $_{\text{information type}}$ = {(**confidentiality**, *not applicable*), (**integrity**, *low*), (**availability**, *low*)}

Security Category $_{\text{information system}}$ = {(**confidentiality**, *moderate*), (**integrity**, *moderate*), (**availability**, *low*)}

TIP

The types of activities [8] associated with the assignment of a system security category based on the aggregate of information types include:

- Reviewing identified security categorizations for the aggregate of information types.
- Determining the system security categorization by identifying the security impact level high-water mark for each of the security objectives (confidentiality, integrity, availability): SC System X={(confidentiality, impact), (integrity, impact), (availability, impact)}.
- Adjusting the security impact level high-water mark for each system security objective (as necessary).
- Assigning the overall information system impact level based on the highest impact level for the system security objectives (confidentiality, integrity, availability).
- Following the agency's oversight process for reviewing, approving, and documenting all determinations or decisions.

Determine the System Security Impact Level

The final step in the security categorization process is the assignment of an overall security impact level[56] to the information system using the high-water mark.[57] As an example, the security categorization for the following information system would be *Moderate*.

However, similar to the focus on adjusting security categories for information types, the system security objectives can also be adjusted based on the application of several factors such as the aggregation of different types of data (change of the information sensitivity when integrated with other information types) and critical

[56] From Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick, J. NIST Special Publication (SP) 800-60 Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Maryland: National Institute of Standards and Technology; 2008. *"Impact levels (plural), as used here, refers to low, moderate, high, or not applicable values assigned to each security objective (i.e. confidentiality, integrity, and availability) used in expressing the security category of an information type or information systems. The value of not applicable only applies to information types and not to information systems."*

[57] The highest values from among the security objectives from all information types identified.

Table 5.3 Potential Impact Levels [7]

	Potential Impact		
Security Objective	***Low***	***Moderate***	***High***
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals	The unauthorized modification or destruction of information could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals
Availability Ensuring timely and reliable access to and use of information [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals	The disruption of access to or use of information or an information system could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals

TIP

For legacy information systems (including service providers), a gap analysis [12] can be performed as follows:

1. Confirm (or update) the security categorization;
2. Review the existing security plan (considering any updates to the security categorization); and
3. Implement security controls in the updated security plan with specific attention given to any new security controls or enhancements.

system functionality (interconnection of the system with other information systems and the dependence of the information by other information systems to support a specific mission/business function). In addition, there are other factors that relate to the specific context of the information and the information system (e.g., information that would be subject to privacy laws and policies, supporting infrastructure that stores, processes, or transmits (flows) information within or across the network or system components).

Security Control Selection

The security control selection is the next step in the NIST RMF (*Step 2*) and includes three major tasks, included in Table 5.4. In this section, most of the focus will be spent on the second and third task. The second task includes the security control selection process which begins with the initial security control baseline[58] and concludes with a final set of security controls that will be implemented.[59] The third task involves the development of a strategy to monitor the selected security controls as part of an information security continuous monitoring (ISCM)[60] program.

The initial security control baseline consists of a minimum set of security requirements derived from among the 17[61] security-related areas included in Table 5.5. "The 17 areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems" [13]. The determination of which requirements from within each area will be included in the initial security control baseline is based on the impact level for the information system following the security categorization process in the NIST RMF (*Step 1*).

[58] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Baseline controls are the starting point for the security control selection process."*

[59] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"For legacy systems, some or all of the security controls selected may already be implemented."*

[60] From Dempsey, K., Chawla, N., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2011. *ISCM is "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions."*

[61] The PM family of security controls relates to an organizational information security program, and therefore they may not be specific to only one information system.

Table 5.4 NIST RMF Step 2 Activities [3]

Task	Name	Activities	References
2-1	Common control identification	• Identify the security controls that are provided by the organization as common controls for organizational information systems • Document the controls in a security plan (or equivalent document)	• FIPS 199 • FIPS 200 • NIST SP 800-18 • NIST SP 800-30 • NIST SP 800-53 • CNSS Instruction 1253
2-2	Security control selection	• Select the security controls for the information system • Document the controls in the security plan	• FIPS 199 • FIPS 200 • NIST SP 800-18 • NIST SP 800-30 • NIST SP 800-53 • CNSS Instruction 1253
2-3	Monitoring strategy	• Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information system and its environment of operations	• NIST SP 800-30 • NIST SP 800-39 • NIST SP 800-53 • NIST SP 800-53A • NIST SP 800-117 • NIST SP 800-126 • NIST SP 800-128 • NIST SP 800-137 • CNSS Instruction 1253
2-4	Security plan approval	• Review and approve the security plan	• NIST SP 800-18 • NIST SP 800-30 • NIST SP 800-53 • CNSS Instruction 1253

The security control selection process includes multiple steps beginning with the selection of the initial security control baseline. Once the baseline has been determined, the next step involves tailoring the initial security control baseline. As illustrated in Figure 5.9, to ensure the resulting security controls required for the information system achieve cost-effective, risk-based security, and any rationale and tailoring is an integral

Table 5.5 Security Control Families [6]

Class[a]	Acronym	Name	Activities
Management	PM	Program management	Organization-wide information security program management controls that are independent of any particular information system and are essential for managing information security programs (e.g., Information Security Program Plan)
Management	RA	Risk assessment	Assessing the risk to organizational operations, assets, and individuals resulting from the operation of information systems, and the processing, storage, or transmission of information
Management	PL	Planning	Developing, documenting, updating, and implementing security plans for systems
Management	SA	System and services acquisition	Allocating resources to protect systems, employing SDLC processes, employing software usage and installation restrictions, and ensuring that third-party providers employ adequate security measures to protect outsourced information, applications, or services
Management	CA	Certification and accreditation and security assessments	Assessing security controls for effectiveness, implementing plans to correct deficiencies and to reduce vulnerabilities, authorizing the operation of information systems and system connections, and monitoring system security controls
Operational	PS	Personnel security	Ensuring that individuals in positions of authority are trustworthy and meet security criteria, ensuring that information and information systems are protected during personnel actions, and employing formal sanctions for personnel failing to comply with security policies and procedures
Operational	PE	Physical and environmental protection	Ensuring that individuals in positions of authority are trustworthy and meet security criteria, ensuring that information and information systems are protected during personnel actions, and employing formal sanctions for personnel failing to comply with security policies and procedures
Operational	CP	Contingency planning	Establishing and implementing plans for emergency response, backup operations, and post-disaster recovery of information systems
Operational	CM	Configuration management	Establishing baseline configurations and inventories of systems, enforcing security configuration settings for products, monitoring and controlling changes to baseline configurations and to components of systems throughout their SDLC
Operational	MA	Maintenance	Performing periodic and timely maintenance of systems, and providing effective controls on the tools, techniques, mechanisms, and personnel that perform system maintenance

Table 5.5 Security Control Families [6] (*continued*)

Class[a]	Acronym	Name	Activities
Operational	SI	System and information integrity	Identifying, reporting, and correcting information and system flaws in a timely manner, providing protection from malicious code, and monitoring system security alerts and advisories
Operational	MP	Media protection	Protecting information in printed form or on digital media, limiting access to information to authorized users, and sanitizing or destroying digital media before disposal or reuse
Operational	IR	Incident response	Establishing operational incident handling capabilities for information systems, and tracking, documenting, and reporting incidents to appropriate officials
Operational	AT	Awareness and training	Ensuring that managers and users of information systems are made aware of the security risks associated with their activities and of applicable laws, policies, and procedures related to security, and ensuring that personnel are trained to carry out their assigned information security–related duties
Technical	IA	Identification and authentication	Identifying and authenticating the identities of users, processes, or devices that require access to information systems
Technical	AC	Access control	Limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to types of transactions and functions that authorized users are permitted to exercise
Technical	AU	Audit and accountability	Creating, protecting, and retaining information system audit records that are needed for the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity, and ensuring that the actions of individual users can be traced so that the individual users can be held accountable for their actions
Technical	SC	System and communications protection	Monitoring, controlling, and protecting communications at external and internal boundaries of information systems, and employing architectural designs, software development techniques, and systems engineering principles to promote effective security

[a] *NIST SP 800-53 Revision 4 removes the labels that provide a class distinction between security controls as many security controls have management, operational, and technical aspects.*

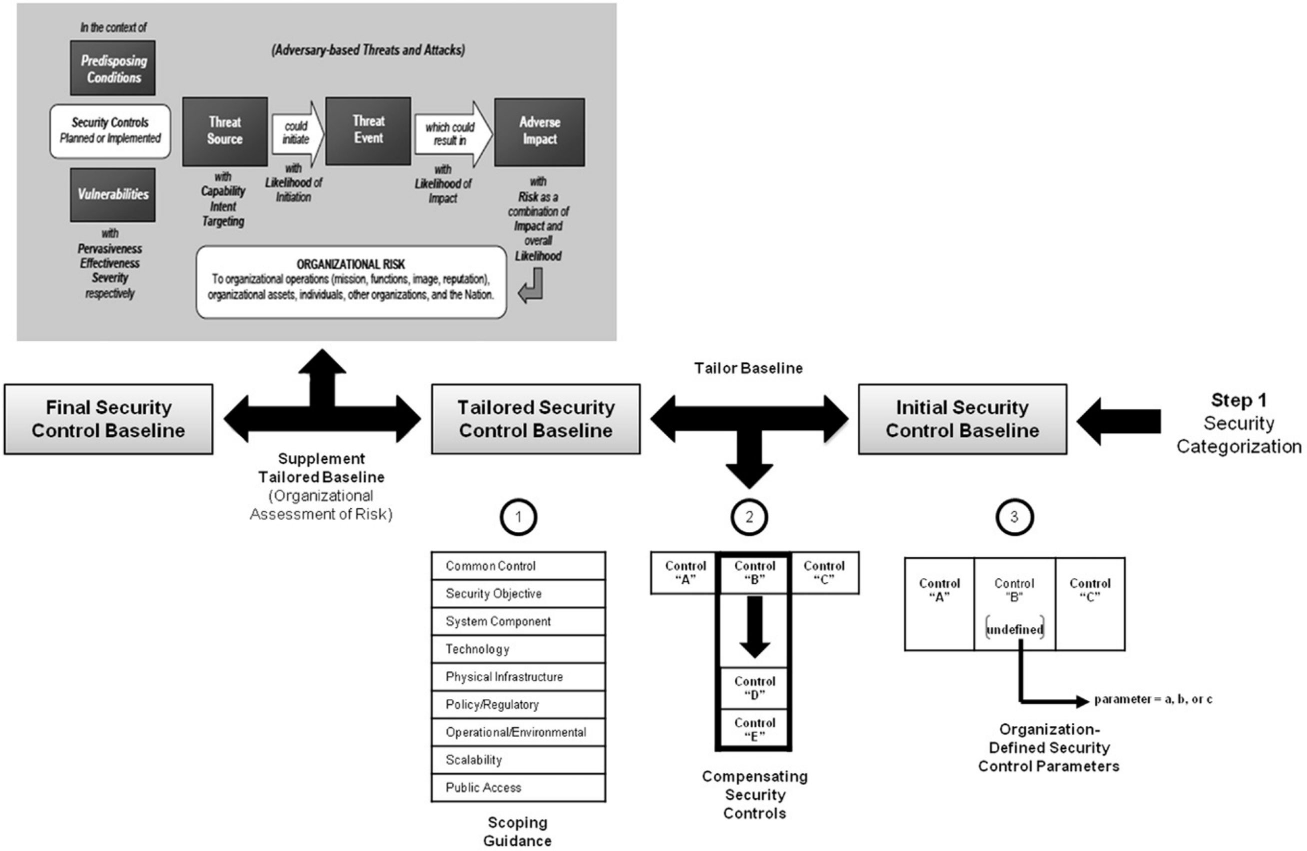

In the context of
Predisposing Conditions
Security Controls Planned or Implemented
Vulnerabilities
with Pervasiveness Effectiveness Severity respectively
(Adversary-based Threats and Attacks)
Threat Source
with Capability Intent Targeting
could initiate
with Likelihood of Initiation
Threat Event
which could result in
with Likelihood of Impact
Adverse Impact
with Risk as a combination of Impact and overall Likelihood
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Final Security Control Baseline
Supplement Tailored Baseline (Organizational Assessment of Risk)
Tailored Security Control Baseline
Tailor Baseline
Initial Security Control Baseline
Step 1 Security Categorization
1
Common Control
Security Objective
System Component
Technology
Physical Infrastructure
Policy/Regulatory
Operational/Environmental
Scalability
Public Access
Scoping Guidance
2
Control "A"
Control "B"
Control "C"
Control "D"
Control "E"
Compensating Security Controls
3
Control "A"
Control "B"
undefined
Control "C"
parameter = a, b, or c
Organization-Defined Security Control Parameters

FIGURE 5.9 Security Controls Selection Process

part of the organization's risk management process.[62,63] In addition, any changes to the baseline need to be supported by documentation[64] that addresses decisions made for adjusting the initial security control baseline such as through an assessment of risk within the information system and operating environment.

Tailoring the Initial Baseline

The tailoring process involves the customization of the initial security control baseline. This process uses three mechanisms to adjust the baseline to more closely align the security control requirements to the actual information system and/or operating environment:

- *Scoping guidance*—specific terms and conditions on the applicability and implementation of specific security controls;
- *Compensating security controls*—management, operational, and technical controls implemented in lieu of an identified security controls in the initial security control baseline;
- *Organization-defined parameters*—parameters applied to portions of a security control to support specific organization requirements or objectives.

In addition, the concept of overlays[65] provides a process for tailoring based on an organizational-specific set of security controls that have been identified to supplement the baseline for a community-wide use or to address specialized requirements, technologies, or unique missions/environments of operation [20]. For example, the Federal Risk and Authorization Management Program (FedRAMP) utilizes the security controls for low- and moderate-impact information systems and contains controls and enhancements above the NIST baseline that addresses the unique elements deemed necessary for the government-wide use of cloud computing [21].

Applying Scoping Considerations

Scoping ensures security requirements are identified for providing an adequate level of protection by providing specific security terms and conditions for addressing the implementation of security controls based on the organization's mission and business processes supported by the information system. In addition, the application of scoping guidance can

[62] The NIST Risk Management Process will be discussed in detail in Chapter 6, Risk Management.

[63] Tailoring decisions should be documented in the security plan (or a related document).

[64] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. "The level of detail required in documenting tailoring decisions in the security control selection process is at the discretion of organizations and reflects the FIPS 199 impact levels of the respective information systems implementing or inheriting the controls."

[65] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"An overlay is a fully specified set of security controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance."*

NOTE

Compensating controls should only be employed if [12]:

- The organization selects the compensating control from NIST Special Publication 800-53, or if an appropriate compensating control is not available, the organization adopts a suitable compensating control from another source;
- The organization provides supporting rationale for how the compensating control delivers an equivalent security capability for the information system and why the related baseline security control could not be employed; and
- The organization assesses and formally accepts the risk associated with employing the compensating control in the information system.

ensure security controls are cost-effectively and efficiently applied by eliminating unnecessary security controls. There are several scoping considerations that can be applied when adjusting the initial security control baseline to the environment of operation:

- Use of common controls;[66]
- Downgrading security controls for those that do not uniquely attribute to high-water mark for the security objectives (i.e., *confidentiality, integrity,* or *availability*);
- Allocation of security controls applicable to specific information system components;
- Removal of security controls that are technology dependent;
- Application of security control for those areas that support the physical infrastructure used to provide direct protection;
- Employment of security controls based on the laws, directives, policies, etc. that govern the information types and the information system;
- Employment of security controls that are consistent with the assumption about the operational environment;
- Implementation of security controls based on the scalability associated with the specific impact level; and
- Application of security controls where public access is granted.

Selecting Compensating Security Controls

Compensation is the function of implementing one or more security controls in lieu of a security control in the initial security control baseline. Although there are many circumstances that could occur where compensation would be required, the most important aspect of using compensation is to have a clear understanding of the risks

[66] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Common controls are security controls that are inherited by one or more organizational information systems."*

associated with not implementing the recommended security control. The compensating security control(s) should provide, at minimum, a comparable level of protection and mitigate any risk introduced through the removal of the control from the initial security control baseline.

Assigning Security Control Parameter Values

Organization-defined parameters are included in portions of security controls to offer flexibility in the implementation. The parameters enable the security control requirements to be completed with specific values that could come from within the organization or as prescribed by federal laws, Executive Orders, directives, and policies that govern the type of information or information system, or other sources such as industry "best practices." In situations where the prescribed parameters are more restrictive, they should be applied to the maximum extent possible. In addition, if there are variations to recommended parameters, the differences should be documented to ensure the organization has some understanding of the risk and can apply the necessary compensating controls to mitigate risks that are determined to be unacceptable.

Supplementing the Tailored Baseline

Once the initial baseline has been tailored (if necessary), the tailored baseline (or initial baseline if no tailoring was performed) should be reviewed to ensure it provides the adequate protection and any identified organization risk[67] that exists is mitigated. Enhancing security control baselines by selecting additional security controls or supplementing the baseline security controls with enhancements can be accomplished through the definition of requirements or conducting a gap analysis. Requirements definition involves an evaluation of the risk assessment to establish requirements. Therefore, a gap analysis focuses on characterizing the security requirements through an assessment of the existing security capabilities and determining the types of threats that can likely be prevented. As an example, Figure 5.10 provides an illustration of the framework in which "to effectively withstand cyber attacks from adversaries with the stated capabilities or attack potential, the organization strives to achieve a certain level of security capability or cyber preparedness"[68] [12]. However, in either approach, the goal is to use the information from the analysis to identify security

[67] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *The risk assessment provides important inputs to determine the sufficiency of the security controls.*

[68] Cyber preparedness, in general, is the process of characterizing the threat source's intent and motivations to ensure a commensurate level of security capabilities exists to defend against an attack. NIST Special Publication (SP) 800-30 Revision 1, Appendix D ("Threat Sources") provides an example of a threat taxonomy that can be used as a starting point for building a tailored list of threat sources.

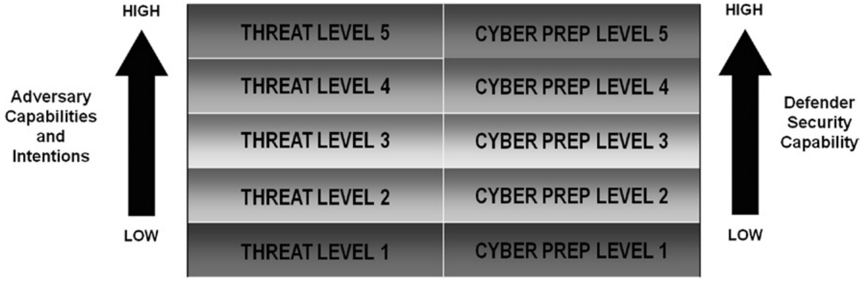


FIGURE 5.10 Cyber Preparedness [15]

controls and/or enhancements which will be required to attain the appropriate level of preparedness.

Documenting the Tailoring and Supplementation Process

The rationale for the decisions made throughout the tailoring and supplementation process resulting in an adjustment to the initial security control baseline should be documented. Table 5.6 provides an example of the type of information that should be used when tailoring the security control baseline and for determining if any impacts would occur to a federal agency's mission or business based on the changes in the security control baseline. In addition, the information documented could be used by the authorizing official to make a credible, risk-based decision as part of the authorization step of the NIST RMF (*Step 5*). This information is also important for understanding any risk-based decisions that were made so they can be evaluated if any changes occur during the monitoring step of the NIST RMF (*Step 6*).

Table 5.6 Documenting Tailoring Rationale [6]

Control	Tailoring Guidance	Rationale
[Control Number and Name]	**Select tailoring guidance** {*Common Control*}, {*Security Objective*}, {*System Component*}, {Technology}, {*Physical Infrastructure*}, {*Policy/Regulatory*}, {*Operational/Environmental*}, {*Scalability*}, or {*Public Access*}	[Scoping Consideration]: *rationale*
[Control Number and Name]	**Compensating control**	[Compensating control(s)]: *rationale*
[Control Number and Name]	**Supplemental control**	[Risk]: *rationale*

Continuous Monitoring Strategy

Continuous monitoring planning[69] starts with the development of a continuous monitoring strategy[70] during the security control selection process. During this step, the strategy focuses on defining "how changes to the information system will be monitored and how the security impact analyses will be conducted" [3]. In addition, the strategy includes the identification of any volatile security controls and the frequency at which those security controls should be monitored over time. This also requires establishing the approach for conducting assessments (e.g., automated techniques and tools such as Secure Content Automation Protocol (SCAP),[71] architectures to support dynamic monitoring and reporting such as the Continuous Asset Evaluation, Situational, Awareness, and Risk Scoring (CAESARS)[72] Framework Extension (FE),[73] and manual assessments).

Allocating Security Controls

Defining the information system boundary[74] during the security categorization process requires understanding the scope of protection for the system components allocated to the information system and interfaces between interconnected systems. This boundary definition activity is critical for fully understanding and clarifying any

[69] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The implementation of a robust continuous monitoring program allows an organization to understand the security state of the information system over time and maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and mission/business functions."*

[70] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The strategy defines how changes to the information system will be monitored, how security impact analyses will be conducted, and the security status reporting requirements including recipients of the status reports."*

[71] *Security Content Automation Protocol (SCAP)*. Available from: http://scap.nist.gov.

[72] From US Department of Homeland Security (DHS), National Cyber Security Division (NCSD), Federal Network Security (FNS) [Internet]. Washington: US Department of Homeland Security [cited 2011 Dec 13]. Available from: http://www.dhs.gov/files/publications/gc_1285952885143.shtm. *"CAESARS represents a solution for making assessments on a continuous or nearly continuous basis; this is a prerequisite for moving IT security management from isolated assessments, supporting infrequent authorization decisions, to continuous risk management."*

[73] NIST Interagency Report (IR) 7756 (Draft), *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture*. Available from: http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf.

[74] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Well-defined boundaries establish the scope of protection for organizational information systems (i.e. what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes."*

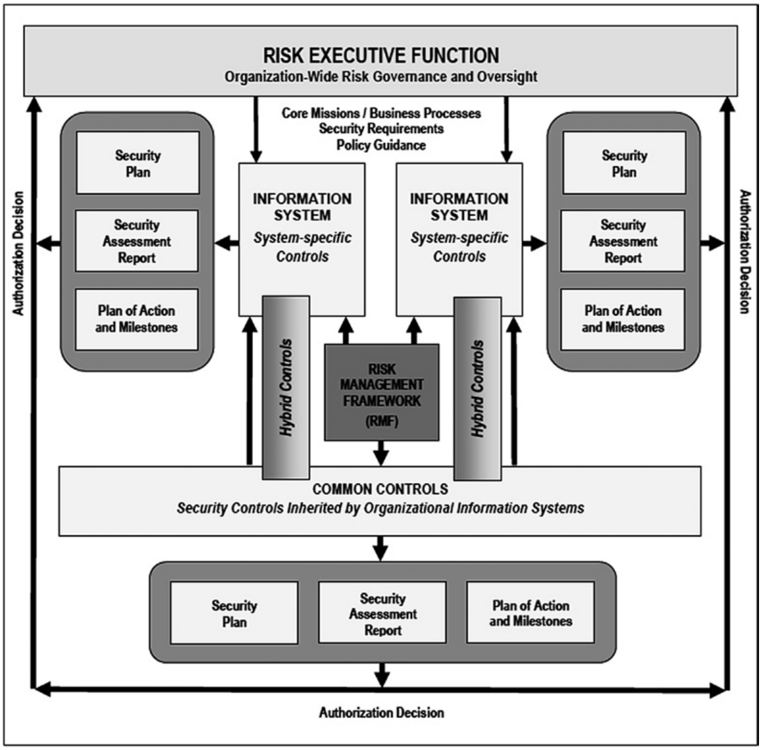

RISK EXECUTIVE FUNCTION
Organization-Wide Risk Governance and Oversight
Core Missions / Business Processes
Security Requirements
Policy Guidance
Security Plan
Security Assessment Report
Plan of Action and Milestones
INFORMATION SYSTEM
System-specific Controls
INFORMATION SYSTEM
System-specific Controls
Security Plan
Security Assessment Report
Plan of Action and Milestones
Authorization Decision
Authorization Decision
Hybrid Controls
RISK MANAGEMENT FRAMEWORK (RMF)
Hybrid Controls
COMMON CONTROLS
Security Controls Inherited by Organizational Information Systems
Security Plan
Security Assessment Report
Plan of Action and Milestones
Authorization Decision

FIGURE 5.11 Security Control Allocation [3]

shared roles and responsibilities for implementing, monitoring, and assessing security controls allocated[75] as part of the security control selection process. However, clarifying roles and responsibilities is not only important as it relates to establishing the ownership of the security controls, but can also help with determining the security-related information that needs to be shared when communicating[76] between security control owners. Although only a conceptual model, Figure 5.11 does provide

[75] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Allocation is a term used to describe the process an organization employs: (i) to determine whether security controls are defined as system-specific, hybrid, or common; and (ii) to assign security controls to specific information system components responsible for providing a particular security capability (e.g. router, server, remote sensor)."*

[76] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Communication regarding the security status of common (inherited) controls is essential irrespective of whether the common control provider is internal or external to the organization."*

a high-level illustration of the potential flow of information when allocating security controls, and when assigning ownership for common capabilities that support more than one information system (i.e., common controls or portions of controls in a hybrid controls situation). In addition, establishing a definition of the authorization boundary and the level of control of the resources can provide a clear delineation of the specific security controls being inherited such as system components which may be used by an organization, but may be outside the direct control of the authorizing official. For security control allocation to be successful, in most cases it requires building trusted relationships based on the sharing of evidence that specific security controls are implemented correctly and operating effectively, including any assessment results (or a summary) and information collected as part of an ongoing continuous monitoring program. The sharing of information ensures changes that could impact the information system inheriting the common controls (or hybrid portions) are understood and any identified risks through the risk management process can be accepted or mitigated through the application of compensating controls.

Decomposition

Decomposition enables complex information systems and security controls to be allocated among more manageable subsystems,[77] thereby enabling subsystems to be viewed independently[78] and security controls can be allocated based on security objectives or common capabilities or functions in the information system architecture. This type of approach could also more effectively focus security controls to achieve a more cost-effective application of the risk management processes such as conducting assessments[79] and ongoing continuous monitoring. Subsystems may be dynamic, where they may be provisioned or de-provisioned rapidly as required, or may not reside within the information system but only at a specific point in the information system lifecycle. In other cases, the subsystems may be controlled and

[77] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"A subsystem is a major subdivision of an information system consisting of information, information technology, and personnel that perform one or more specific functions."*

[78] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Separately categorizing each subsystem does not change the overall categorization of the information system."*

[79] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The organization can: (i) issue a single authorization for the entire complex information system (to include bundling assessment results from individual subsystem assessments and any additional assessment results at the system level); or (ii) implement a strategy for managing the risk associated with connecting separately authorized information systems when viewed as a system of systems."*

managed by a service provider outside of the authorization boundary or outside of the control of the organization. In these situations, establishing subsystems enables parts of the information system that are more volatile or not within the control of the federal agency or service provider to be monitored differently based on the federal agency's assurance requirements to ensure required security controls continue to operate at an acceptable level of risk over time.

Security Controls Implementation

In this step of the NIST RMF (*Step 3*), both the tasks included in Table 5.7 will be covered together due to their close relationship (i.e., implementation of the security controls and documentation of their implementation may occur concurrently). To enable the efficient and cost-effective implementation of security controls, some

Table 5.7 NIST RMF Step 3 Activities [3]

Task	Name	Activities	References
3-1	Security control implementation	• Implement the security controls specified in the security plan	• FIPS 200 • NIST SP 800-30 • NIST SP 800-53 • NIST SP 800-53A • CNSS Instruction 1253
3-2	Security control documentation	• Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs)	• NIST SP 800-18 • NIST SP 800-53 • CNSS Instruction 1253

NOTE

What is the purpose of the system security plan?

"The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system" [3].

knowledge of the existing and target information security architecture[80] may be required. The information security architecture serves to influence security controls allocated to system components within the information system during the security control selection process. In addition, the allocation of security controls should be based on "best practices" focused on identifying specific system components for providing a security capability.

Documenting the security control implementation in the security plan provides a functional description of the security controls (i.e., planned inputs, expected behavior, and expected outputs) both from an organizational perspective (management and operational security controls) and a system perspective (operational and technical security controls). In addition, the security plan documents a description of any inheritance (common security controls), shared ownership (hybrid security controls), and the system-specific security controls allocated to system components within the information system boundary. The level of detail for documenting security controls implementation should commensurate with the impact level assigned to the information system, but should at least provide traceability of decisions prior to and after deployment of the information system and be sufficient to support control assessment [3].

Implementing and Documenting Security Controls

As discussed earlier in the chapter, the integration of security early in the SDLC enables architects and engineers to integrate security controls into the information security architecture[81] by applying overlapping, defense-in-depth protective layers,[82] through the use of security engineering principles,[83] and secure coding methodologies.[84] Additionally, the implementation of risk management activities (e.g., development testing

[80] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"The information security architecture includes an architectural description, the placement/allocation of security functionality, security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface."*

[81] In a legacy information system, a *"gap analysis"* can be used to understand any limitation in the existing information security architecture where security controls are not functioning properly so that corrective actions can be planned and compensating controls can be identified to provide adequate protection for any unacceptable risks.

[82] For information on defense-in-depth protective layers, see the National Security Agency (NSA), Defense in Depth White Paper. Available from: www.nsa.gov/ia/_files/support/defenseindepth.pdf.

[83] For information on the security engineering principle, see NIST SP 800-27 Rev A. Available from: csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.

[84] From US Department of Homeland Security, National Cyber Security Division (NCSD), Strategic Initiatives Branch [Internet]. Washington: US Department of Homeland Security [cited 2011 Dec 15]. Available from: https://buildsecurityin.us-cert.gov/bsi/home.html. *"Build Security In is a collaborative effort that provides practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development."*

and evaluation[85]) ensures information security planning is performed in parallel with the information system development to identify any weaknesses and deficiencies that will need to be mitigated, thereby maximizing the reuse of the assessment results in later phases of the SDLC and achieving a more cost-effective balance between the implementation of security controls and the management of risk. In addition, security control allocation, both between the security control owners (e.g., common control providers) and information system components, requires identifying any dependencies from the security control selection process. This activity is essential to ensure any changes to the planned security controls resulting from the infeasibility or impracticability of their implementation can be updated in the security plan documentation to capture any risk-based decision-making and accurately describe compensating security controls that will be implemented to minimize the impact associated with unacceptable risks.

Security Controls Assessment

The security controls implemented and documented in the previous steps are essential components for conducting an effective assessment.[86] The security controls assessment step in the NIST RMF (*Step 4*) involves the preparation, execution, and reporting of the security controls effectiveness in the information system. This section will summarize the assessment-related tasks in Table 5.8. The assessment tasks are dependent on the close collaboration and cooperation of the security assessor[87] and the organization to ensure there is an appropriate level of depth[88] and coverage[89]

[85] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Developmental testing and evaluation activities include, for example, design and code reviews, application scanning, and regression testing."*

[86] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Partial assessments of security controls can be conducted in the initial phases of system development life cycle to promote early detection of weakness and deficiencies and a more cost-effective approach to risk mitigation."*

[87] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The individual, group, or organization responsible for conducting a security control assessment."*

[88] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method."*

[89] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g. types of objects to be assessed and the number of objects to be assessed by type)."*

Table 5.8 NIST RMF Step 4 Activities [3]

Task	Name	Activities	References
4-1	Assessment preparation	• Develop, review, and approve a plan to assess the security controls	• NIST SP 800-53A
4-2	Security control assessment	• Assess the security controls in accordance with the assessment procedures defined in the security assessment plan	• NIST SP 800-53A • NIST SP 800-115
4-3	Security assessment report	• Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment	• NIST SP 800-53A
4-4	Remediation actions	• Conduct the initial remediation actions on security controls based on the findings and recommendations of the security assessment report • Reassess remediated control(s), as appropriate	• NIST SP 800-30 • NIST SP 800-53A

applied when evaluating the security controls effective against the organization's identified assurance requirements.[90]

Assessment Preparation

Prior to beginning the assessment activities, expectations should be appropriately set through the development of a security assessment plan. Preparatory activities should be planned together, by the organization undergoing the assessment and the provider conducting the assessment, to limit any unexpected issues and to gain a clear understanding of the level of effort required. Figure 5.12 provides an example list of preparatory activities that guide the completion of the assessment plan. In addition, the organization should also provide the security assessor with the following types of information:

- Organizational chart (or description of organizational personnel responsible for security policies and procedures);

[90] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Assurance requirements address the quality of the design, development, and implementation of the security functions in the information system."*

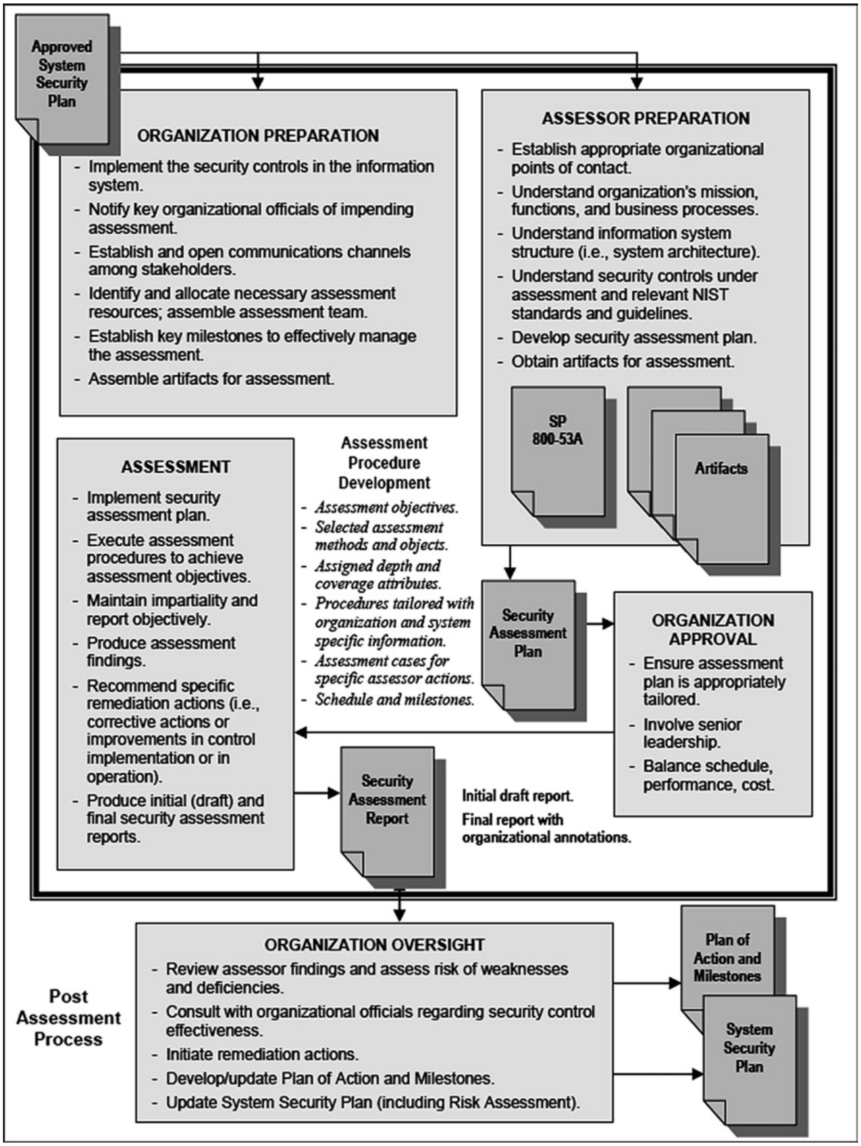

Approved System Security Plan
ORGANIZATION PREPARATION
- Implement the security controls in the information system.
- Notify key organizational officials of impending assessment.
- Establish and open communications channels among stakeholders.
- Identify and allocate necessary assessment resources; assemble assessment team.
- Establish key milestones to effectively manage the assessment.
- Assemble artifacts for assessment.
ASSESSOR PREPARATION
- Establish appropriate organizational points of contact.
- Understand organization's mission, functions, and business processes.
- Understand information system structure (i.e., system architecture).
- Understand security controls under assessment and relevant NIST standards and guidelines.
- Develop security assessment plan.
- Obtain artifacts for assessment.
SP 800-53A
Artifacts
ASSESSMENT
- Implement security assessment plan.
- Execute assessment procedures to achieve assessment objectives.
- Maintain impartiality and report objectively.
- Produce assessment findings.
- Recommend specific remediation actions (i.e., corrective actions or improvements in control implementation or in operation).
- Produce initial (draft) and final security assessment reports.
Assessment Procedure Development
- Assessment objectives.
- Selected assessment methods and objects.
- Assigned depth and coverage attributes.
- Procedures tailored with organization and system specific information.
- Assessment cases for specific assessor actions.
- Schedule and milestones.
Security Assessment Plan
ORGANIZATION APPROVAL
- Ensure assessment plan is appropriately tailored.
- Involve senior leadership.
- Balance schedule, performance, cost.
Security Assessment Report
Initial draft report.
Final report with organizational annotations.
Post Assessment Process
ORGANIZATION OVERSIGHT
- Review assessor findings and assess risk of weaknesses and deficiencies.
- Consult with organizational officials regarding security control effectiveness.
- Initiate remediation actions.
- Develop/update Plan of Action and Milestones.
- Update System Security Plan (including Risk Assessment).
Plan of Action and Milestones
System Security Plan

FIGURE 5.12 Security Controls Assessment Process [17]

- Policies and procedures that relate to the information system;
- Organizational chart (or description of organizational personnel responsible for security control implementation); and
- Artifacts, where available, that provide an understanding of security controls such as the security plan, risk assessment, continuous monitoring plan, plan

of action and milestones (POA&Ms), accreditation decision letter (if already under an existing accreditation), privacy impact assessment (PIA), contingency plan, configuration management plan, security configuration checklists, and/or system interconnection agreements (ISA, MOU, contracts, etc.).

Security Assessment Plan

Planning activities are critical for the success of the security assessment. The security assessment plan (SAP), [91] developed by the security assessor, should be reviewed and approved by the organization based on an agreement of what is in scope for the assessment. Similar to *Step 2,* where the organization selects, tailors, and supplements security controls to be implemented, the security assessor should also perform similar activities by selecting, tailoring, and supplementing assessment procedures that address specific assurance requirements by the organization.

TIP

Select, Tailor, Customize, Optimize

As a guide, and to improve the effectiveness in executing assessments, an assessor should seek to find ways to save time and money when conducting assessments through the following steps [17]:

- Select assessment methods[92] and objects that match the assurance requirements.
- Select the appropriate depth and coverage attributes.[93]
- Identify common controls to reduce redundancy and duplication of effort.
- Customize security-specific assessment procedures to closely match the operating environment (and utilizing supplemental guidance in the NIST Security Controls Catalog to establish an intent of the security control).
- Identify assessment results that are applicable for reuse (previous assessments) or through more efficiency in sequencing the current assessment.
- Adjust assessment procedures to accommodate external service providers based on contracts or service level agreements.
- Develop assessment procedures[94] for custom security controls.
- Identify areas where assessment procedures can be combined and consolidated to maximize cost savings without compromising quality.

[91] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The security assessment plan provides the objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment."*

[92] Examine, interview, and test.

[93] Basic, focused, and comprehensive.

[94] In situations where security controls not included in Security Control Catalog (NIST Special Publication (SP) 800-53, Appendix F) were included in the security control baseline, the assessor may have to develop custom security assessment procedures. In these situations, NIST Special Publication (SP) 800-53A can be used as a guide.

Assessing Security Controls

Conducting security assessments,[95] which will be discussed in more detail in later chapters, is described briefly in this section. The security assessment execution is primarily organized and executed by the security assessor, with the organization's support. Therefore, the key focus will be on making the assurance case.[96]

When conducting the security assessment, the security assessor needs to obtain evidence[97] to facilitate the security assessor in making an objective determination of security control effectiveness, based on the criteria (i.e., expect input, behavior, and outcome) identified in the assessment procedures. Since the key focus will be on making the assurance case, the evidence should come directly from the information system or operating environment, or from a third-party evaluation of the product or technology such as a common criteria evaluation.[98] In addition, automated tools and techniques could be used to improve the quality of the security assessment through an increase in the sampling size and coverage.

Reporting Assessment Results

Reporting on the security control assessment results, including any issues, weaknesses and deficiencies, and recommendations, is performed through the security assessment report (SAR).[99] The SAR works together with the security plan (including risk assessment) and POA&Ms to provide an overall picture of the security state and risk posture for the information system. The specific reporting format for security assessment results is organizationally dependent, but should provide enough detail to enable the authorizing official to establish a credible, risk-based decision. In addition to findings, the SAR also includes key recommendations for addressing the findings.[100] Evidence produced during the security assessment should be retained by

[95] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Security control assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system."*

[96] From US Department of Homeland Security, National Cyber Security Division (NCSD), Strategic Initiatives Branch [Internet]. Washington: US Department of Homeland Security [cited 2011 Dec 17]. Available from: https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/643-BSI.html. *"An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system holds, i.e. is assured."*

[97] Supporting information about the claims of security controls implemented within information system.

[98] For more information on the Common Criteria Evaluation and Validation Scheme (CCEVS), see http://www.niap-ccevs.org/.

[99] The security assessment report is one component of the security authorization package that is used by the authorizing official to make an authorization decision.

[100] Depending on when the security assessment was performed in the SDLC (e.g., development/test), initial reports of findings of a *"delta"* could be resolved during the information system development.

the organization for reuse in future security assessment-related activities either through manual or automated consumption.[101]

Information System Authorization

The next step in the NIST RMF (*Step 5*) concludes with an authorization decision[102] for the information system to operate (or continue to operate, for legacy systems). This section will present the tasks outlined in Table 5.9, with primary emphasis being placed on planning corrective actions and the authorization process.

Corrective Action Planning

The POA&Ms[103] receive input from the SAR, and is one of three key documents presented in the authorization package to the authorizing official. The POA&Ms include a set of tasks focused on correcting weaknesses or deficiencies discovered during the security controls assessment,[104] or security testing (e.g., periodic vulnerability scanning, penetration testing, etc.). In addition, POA&Ms document corrective actions for security weaknesses and deficiencies found during other types of reviews done by, for, or on behalf of the federal agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments [18].

[101] From Cloud Security Alliance (CSA), CloudAudit Working Group [Internet]. Washington: Cloud Security Alliance [cited 2011 Dec 19]. Available from: https://cloudsecurityalliance.org/wp-content/uploads/2011/12/GRC-Stack-CSA-Congress-2011-part-1.pptx. *Automated emerging specifications such as CloudAudit can be used to provide "a structure for organizing assertions and supporting documentation for specific controls across different compliance frameworks in a way that simplifies discovery by humans and tools."*

[102] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The security authorization decision indicates to the information system owner whether the system is: (i) authorized to operate; or (ii) not authorized to operate."*

[103] From Daniels, M. Office of Management and Budget (OMB) Memorandum 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones. Washington: Executive Office of the President, Office of Management and Budget; 2001. *"A plan of action and milestones (POA&M) is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones."*

[104] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"All security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail."*

Table 5.9 NIST RMF Step 5 Activities [3]

Task	Name	Activities	References
5-1	Plan of action and milestones	• Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation action taken	• OMB M-02-01 • NIST SP 800-30 • NIST SP 800-53A
5-2	Security authorization package	• Assemble the security authorization package • Submit the package to the authorizing official for adjudication	
5-3	Risk determination	• Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation	• NIST SP 800-30 • NIST SP 800-39
5-4	Risk acceptance	• Determine if the risk to organizational operation, organizational assets, individuals, other organizations, or the Nation is acceptable	• NIST SP 800-53A

Developing a Risk Mitigation Strategy

A strategy for risk mitigation[105] planning is important when prioritizing corrective actions as part of an organization-wide risk management function. The prioritization[106] should take input from other activities within the NIST RMF, such as security categorization. In addition, other inputs can also influence the risk mitigation strategy, such as the security controls (i.e., where the security weaknesses or deficiencies exist), impacts of the weaknesses and deficiencies on the overall security state of the information system, and the risk mitigation approach used by the organization to address weaknesses and deficiencies [3].

[105] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process."*

[106] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"A risk assessment guides the prioritization process for items included in the plan of action and milestones."*

Documenting POA&Ms

The authorizing official uses POA&Ms as an oversight management tool for tracking corrective actions for a specific information system. In addition, the organization can also use consolidated POA&Ms from across all of the information system to identify common weaknesses and deficiencies to effectively allocate resources for organization-wide security improvements. Therefore, POA&Ms should provide enough details[107] to enable the organization to identify, assess, prioritize, and monitor the correction of weaknesses and deficiencies both in federal and contractor systems.[108] POA&M details[109] should include:

- Brief description of the weakness.[110]
- Identity of the organization held responsible for resolving the weakness.
- Estimated funding resources required to resolve the weakness.
- Scheduled completion date for resolving the weakness.
- Key milestones[111] with completion dates.
- Milestone changes.
- The source of the weakness.
- Status.[112]

[107] From Daniels, M. Office of Management and Budget (OMB) Memorandum 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones. Washington: Executive Office of the President, Office of Management and Budget; 2001. *OMB has developed POA&M guidance which provides specific instructions and examples for the POA&Ms.*

[108] From Bolten, J. Office of Management and Budget (OMB) Memorandum 04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act. Washington: Executive Office of the President, Office of Management and Budget; 2004. *The agency is responsible for ensuring the contractor corrects weaknesses discovered through self-assessments and independent assessments. Any weaknesses are to be reflected in the agency's POA&M.*

[109] From Bolten, J. Office of Management and Budget (OMB) Memorandum 04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act. Washington: Executive Office of the President, Office of Management and Budget; 2004. *The exact format prescribed in the POA&M examples in M-04-25 are no longer required, but, all of the associated data elements must be included in the POA&Ms.*

[110] From Daniels, M. Office of Management and Budget (OMB) Memorandum 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones. Washington: Executive Office of the President, Office of Management and Budget; 2001. "*Description of the weaknesses. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. Where it is necessary to provide more sensitive data, the POA&M should note the fact of its special sensitivity*."

[111] From Daniels, M. Office of Management and Budget (OMB) Memorandum 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones. Washington: Executive Office of the President, Office of Management and Budget; 2001. *A milestone will identify specific requirements to correct an identified weakness.*

[112] From Daniels, M. Office of Management and Budget (OMB) Memorandum 02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones. Washington: Executive Office of the President, Office of Management and Budget; 2001. *Ongoing or completed. "Completed" should be used only when a weakness has been fully resolved and the corrective action has been tested. Include the date of completion.*

Security Authorization Approaches

The security authorization process is based on three different approaches.[113] The first, and most commonly used, is the traditional approach, which involves only *one* authorizing official. In this approach, a single authorizing official has both the responsibility and accountability for accepting security risks.

Next is the joint authorization[114] approach, which includes a shared interest, usually between multiple authorizing officials because the information system ties directly into the strategic mission or business processes. In this approach, the authorizing officials are collectively responsible and accountable for accepting the security risks.

The final approach is used when the mission or business processes are supported by more than one federal agency. This approach is known as the leveraged authorization approach and can be used to authorize an information system, commonly a shared service,[115] that can be used by more than one agency based on the original authorization package without requiring reauthorization by the leveraging organization.

Due to the complexity in implementing the leveraged authorization approach, it is the one used least often of the three, but offers the most cost savings.[116] The leveraging organization, usually through an assigned authorizing official, leverages the original authorization[117] by accepting the risks, and assesses only those additional

[113] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *Organizations can choose from three different approaches when planning for and conducting security authorizations to include: (i) an authorization with a single authorizing official; (ii) an authorization with multiple authorizing officials; or (iii) leveraging an existing authorization*.

[114] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *Collaborating on the security categorization, selection of security controls, plan for assessing the controls to determine effectiveness, plan of action and milestones, and continuous monitoring strategy, is necessary for a successful joint authorization*.

[115] From Office of Management and Budget (OMB). Federal Information Technology Shared Services Strategy. Washington: Executive Office of the President, Office of Management and Budget; 2012. *"A function that is provided for consumption by multiple organizations within or between Federal Agencies."*

[116] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The leveraged authorization approach provides opportunities for significant cost savings and avoids a potentially costly and time-consuming authorization process by the leveraging organization."*

[117] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"When reviewing the authorization package, the leveraging organization considers risk factors such as the time elapsed since the authorization results were produced, the environment of operation (if different from the environment of operation reflected in the authorization package), the criticality/sensitivity of the information to be processed, stored, or transmitted, as well as the overall risk tolerance of the leveraging organization."*

requirements beyond the original security control baseline established by the original.[118] For example, if the leveraging organization determines there is insufficient information in the authorization package or inadequate security measures in place for establishing an acceptable level of risk, the leveraging organization may negotiate for additional security measures[119] and/or security-related information [3].

Another option that may be used by an organization when multiple instances of the same information system (or subsystem) are deployed in a number of different operational environments is the application of a type authorization [3]. In a type authorization a single authorizing package is used to reflect a common view for all of the instances deployed across all locations where the information system is hosted (also known as site-specific controls[120]).

Security Authorization Process

The security authorization process is the most involved step in the NIST RMF (*Step 5*) because it requires the direct or indirect input from each of the previous steps in the NIST RMF (*categorization*, *security control selection*, *security control implementation*, and *security control assessment*) to make the authorization decision. This process begins with the assembly of the authorization package, where the key and supporting documents needed to make the authorization decision are prepared. After the security authorization package has been assembled, the determination of risk involves an analysis of information gathered from across the organization to provide the authorizing official with enough credible information to support a risk-based decision.

The authorization package includes both key and supporting documents.[121] Figure 5.13 illustrates the three key minimum documents that are required by the

[118] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The term owning organization refers to the federal agency or subordinate organization that owns the authorization package."*

[119] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Additional security measures may include, for example, increasing the number of security controls, conducting additional assessments, implementing compensating controls, or establishing constraints on the use of the information system or services provided by the system."*

[120] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Site-specific controls are typically implemented by an organization as common controls."*

[121] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The authorizing official determines what additional supporting documentation or references may be required to be included in the authorization package."*

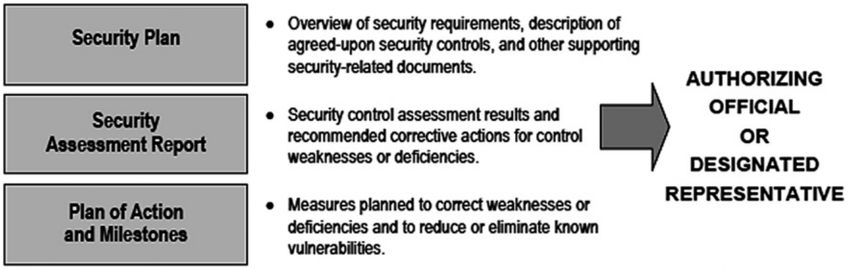

Security Plan
Security Assessment Report
Plan of Action and Milestones
Overview of security requirements, description of agreed-upon security controls, and other supporting security-related documents.
Security control assessment results and recommended corrective actions for control weaknesses or deficiencies.
Measures planned to correct weaknesses or deficiencies and to reduce or eliminate known vulnerabilities.
AUTHORIZING OFFICIAL OR DESIGNATED REPRESENTATIVE

FIGURE 5.13 Security Authorization Package [3]

authorizing official: *security plan*, *SAR*, and *POA&Ms*. These three documents are considered the most accurate representation of the security state of the information system and are based on information derived from activities performed throughout the execution of the NIST RMF.

For security controls inherited in whole or in part by another organization (common control provider) or an external service provider, security risk–related information[122] may be shared with the authorizing official to supplement the authorization package and assist in making an authorization decision. For all of the key documents included in the authorization package, the owner of the information system or provider of common controls generally has the responsibility of the packaging and submitting the security authorization package.

Risk determination is a critical activity in the authorization process that involves reviewing the documents in the security authorization package. During this activity, the authorizing official will likely place significant importance on the security assessment report [22], but will also use information gathered through other risk management activities to understand the organization's overall risk exposure[123] from operating the information system. In addition, the authorizing official will likely rely upon additional input from the other parts of the organization such as the

[122] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Risk-related information includes the criticality of organizational missions and/or business functions supported by the information system and the risk management strategy for the organization."*

[123] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Risk exposure is the degree to which an organization is threatened by the potential adverse effects on organizational operations and assets, individuals, other organizations, or the Nation."*

organization's risk executive[124] and other organizational assessments of risk to assist in making the final determination, in addition to the documents in the security authorization package. "The information system-related security risk information derived from the execution of the NIST RMF is available to the risk executive (function) for use in formulating and updating the organization-wide risk management strategy" [3].

The risk determination concludes in a final determination of an authorization decision as defined in Table 5.10. The authorization decision is achieved through a balance of the security considerations identified through the execution of the NIST RMF, with mission and operational needs for the information system [3]. The security considerations are based on the contents of the authorization package, input from the risk executive, and any other supporting information as determined by the authorizing official.

After the final authorization decision has been made, the decision is communicated to the system owner or common controls provider. The authorization decision document includes not only the authorization decision, but may also include any applicable terms and conditions[125] and a termination date. As an alternative, instead of establishing a termination date (time-drive reauthorizations[126]), the organization could also require the implementation of a continuous monitoring program (event-driven reauthorization[127]) that provides the capability to continuously make risk

[124] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success."*

[125] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The terms and conditions for the authorization provide a description of any limitations or restrictions placed on the operation of the information system or the implementation of common controls that must be followed by the system owner or common control provider."*

[126] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Time-driven reauthorizations occur when the authorization termination date is reached."*

[127] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Event-driven reauthorizations can occur when there is a significant change to an information system or its environment of operation."*

NOTE

As discussed in OMB Memorandum 11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, OMB waived the requirements for a reauthorization every three years.

20. Is a security reauthorization still required every three years or when an information system has undergone significant change as stated in OMB Circular A 130?[128]

No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. Continuous monitoring programs thus fulfill the three year security reauthorization requirement, so a separate re-authorization process is not necessary. In an effort to implement a more dynamic, risk-based security authorization process, agencies should follow the guidance in NIST Special Publication 800-37, Revision 1. Agencies should develop and implement continuous monitoring strategies for all information systems. Agency officials should monitor the security state of their information systems on an ongoing basis with a frequency sufficient to make ongoing risk-based decisions on whether to continue to operate the systems within their organizations. Continuous monitoring programs and strategies should address: (i) the effectiveness of deployed security controls; (ii) changes to information systems and the environments in which those systems operate; and (iii) compliance to federal legislation, directives, policies, standards, and guidance with regard to information security and risk management. Agencies will be required to report the security state of their information systems and results of their ongoing authorizations through CyberScope in accordance with the data feeds defined by DHS.

determinations and acceptance. For example, "if the maximum authorization period for an information system is three years, then an organization establishes a continuous monitoring strategy for assessing a subset of the security controls employed within and inherited by the system during the authorization period. This strategy allows all security controls designated in the respective security plans to be assessed at least one time by the end of the three-year period" [3].

For an ongoing authorization to be successful,[129] the continuous monitoring program needs to integrate information security and risk management into the organization's SDLC. The continuous monitoring NIST RMF (*Step 6*) is aligned with the NIST SDLC operations and maintenance (O&M) phase. The application of configu-

[128] See Office of Management and Budget (OMB) Circular A-130, Appendix III, http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

[129] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The authorizing official maintains sufficient knowledge of the current security state of the information system (including the effectiveness of the security controls employed within and inherited by the system) to determine whether continued operation is acceptable based on ongoing risk determinations, and if not, which step or steps in the Risk Management Framework needs to be re-executed in order to adequately mitigate the additional risk."*

Table 5.10 Authorization Decisions [3]

Decision	Specification
Authorization to operate	• Acceptance[a] of risk to organizational operations and assets, individuals, other organizations, and the Nation • Issued for an information system or common controls inherited • Authorized for a specified period of time (termination date is established as a condition of authorization) • Includes terms and conditions (*optional*)
Denial of authorization to operate	• Non-acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation • Immediate steps cannot be taken to reduce the risk to an acceptable level (*major weaknesses or deficiencies in security controls*) • Issued for an information system or common controls inherited • All activities halted for operational information systems • Inheritance not approved for common control providers within the organization • Revise the plan of action and milestones to ensure that appropriate measures are taken to correct the identified weaknesses or deficiencies
Authorization rescission	• Special case of a denial of authorization to operate • Specific violation of: • Federal/organizational security policies, directives, regulations, standards, guidance, or practices • The terms and conditions of the original authorization

[a] *From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. "The explicit acceptance of risk is the responsibility of the authorizing official and cannot be delegated to other officials within the organization."*

ration management and control policies and procedures identifies changes to the information system, and any automated tools and techniques employed ensures security controls are continuously assessed for effectiveness. In addition, the use of automation also supports the concept of "near real-time" ongoing authorizations.[130]

[130] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Formal reauthorization actions are avoided in situations where the continuous monitoring process provides authorizing officials the necessary information to manage the potential risk arising from changes to the information system or its environment of operation."*

If a management-driven continuous monitoring strategy is applied during the continuous monitoring step, the authorization decision can be streamlined. For example, if reauthorization actions result in either a time-driven (*termination date*) or event-driven (*significant change*[131]) trigger, and information produced as a result of the ongoing assessment activities continued to demonstrate the effectiveness of the security controls, the only action required for reauthorization might include making updates to the original authorization package and resubmission to the authorizing official for risk acceptance.

Security Controls Monitoring

The final step in NIST RMF (*Step 6*) focuses on those activities that support the ongoing authorization of the information system. Through the integration of risk management in an organization-wide information security continuous monitoring (ISCM) program, the security state can be monitored on an ongoing basis. The discussion on development and maintenance of an ISCM program and on specific types of tools, techniques, and technologies will be presented in more detail in later chapters. Therefore, this section limits the discussion to cover only those activities included in Table 5.11 as they relate to the continuous assessment of security controls and updates to risk management documents to support the ongoing risk determination, mitigation, and acceptance.

Managing information risk on an ongoing basis requires a rigorous organizational continuous monitoring[132] strategy and program designed to maintain a security authorization over an extended period of time. Continuous monitoring is a concept in which the security impacts to changes in the information system and the operating environment are managed and controlled. In addition to conducting security impact analyses, the organization can also use automated tools to provide security status-related information to organizational officials in "near real-time" in order to assist the authorizing official in making cost-effective, risk-based decisions regarding the use and operation of the information system. Through a disciplined approach to continuous monitoring, the organization can more efficiently determine the affects on

[131] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"A significant change is defined as a change that is likely to affect the security state of an information system."*

[132] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The monitoring program allows an organization to: (i) track the security state of an information system on a continuous basis and (ii) maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes."*

Table 5.11 NIST RMF Step 6 Activities [3]

Task	Name	Activities	References
6-1	Information system and environment changes	• Determine the security impact of proposed or actual changes to the information system and its environment of operation	• NIST SP 800-30 • NIST SP 800-53A • NIST SP 800-128
6-2	Ongoing security control assessments	• Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy	• NIST SP 800-53A • NIST SP 800-137
6-3	Ongoing remediation actions	• Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones	• NIST SP 800-30 • NIST SP 800-53 • NIST SP 800-53A • CNSS Instruction 1253
6-4	Key updates	• Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process	• NIST SP 800-118 • NIST SP 800-53 • NIST SP 800-53A • NIST SP 800-137
6-5	Security status reporting	• Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy	• NIST SP 800-53A • NIST SP 800-137
6-6	Ongoing risk determination and acceptance	• Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operation, organizational assets, individuals, other organizations, or the Nation remains acceptable	• NIST SP 800-30 • NIST SP 800-39

Table 5.11 NIST RMF Step 6 Activities [3] (*continued*)

Task	Name	Activities	References
6-7	Information system removal and decommissioning	• Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service	• NIST SP 800-30 • NIST SP 800-53A • NIST 800-64

TIP

An effective organization-wide continuous monitoring program [3] includes:

- Configuration management and control processes.
- Security impact analyses on proposed or actual changes.
- Assessment of selected security controls.
- Security status reporting.
- Active involvement by authorizing officials.

changes to the security state of the information system and the necessary corrective actions and/or risk mitigations that need to be put in place.

Determining Security Impact

Over time, information systems can be susceptible to changes. The application of configuration management and control processes[133] requires documenting[134] and

[133] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program."*

[134] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"It is important to record any relevant information about specific changes to hardware, software, or firmware such as version or release numbers, descriptions of new or modified features/capabilities, and security implementation guidance, or any changes to the environment of operation for the information system (e.g. modifications to hosting networks and facilities, mission/business use of the system, threats), or changes to the organizational risk management strategy."*

assessing the impact[135] on changes (*proposed* or *actual*). The assessment of the impact to the security state of the information throughout the SDLC is an important part of maintaining an ongoing security authorization. However, not all changes (e.g., routine changes or scheduled maintenance) will impact the security state of the information system or the environment. Through a consistent application of configuration management and controls processes similar to Figure 5.14, all changes going through the continuous monitoring process will be required to undergo an assessment of risk to support an ongoing authorization based on an understanding of the impacts to those changes.

Ongoing Security Controls Assessments

The monitoring strategy is developed during the security control selection step of the NIST RMF (*Step 2*). The strategy is focused on establishing criteria[136] for selecting which security controls employed within or inherited by the information system should be monitored as part of the continuous monitoring program. The determination of which security controls to assess and the frequency of monitoring requires obtaining input from a variety of sources [3] to include:

- Risk assessments (including current threat and vulnerability information),
- History of cyber attacks,
- Results of previous security assessments, and
- Operational requirements.

In addition, factors such as security control volatility[137] and POA&Ms[138] can also be useful. For example, "security controls that are subject to the direct effects or side

[135] Johnson, A., Dempsey, K., Ross, R., Gupta, S., Bailey, D. NIST Special Publication (SP) 800-128, Guide for Security-Focused Configuration Management of Information System. Maryland: National Institute of Standards and Technology; 2011. *"Security impact analysis is the analysis conducted by qualified staff within an organization to determine the extent to which changes to the information system affect the security posture of the system."*

[136] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The selection criteria reflect the priorities and importance of the information system to organizational operations and assets, individuals, other organizations, and the Nation."*

[137] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Security control volatility is a measure of how frequently a control is likely to change over time subsequent to its implementation."*

[138] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Security controls identified in the plan of action and milestones are also a priority in the continuous monitoring process, due to the fact that these controls have been deemed to be ineffective to some degree."*

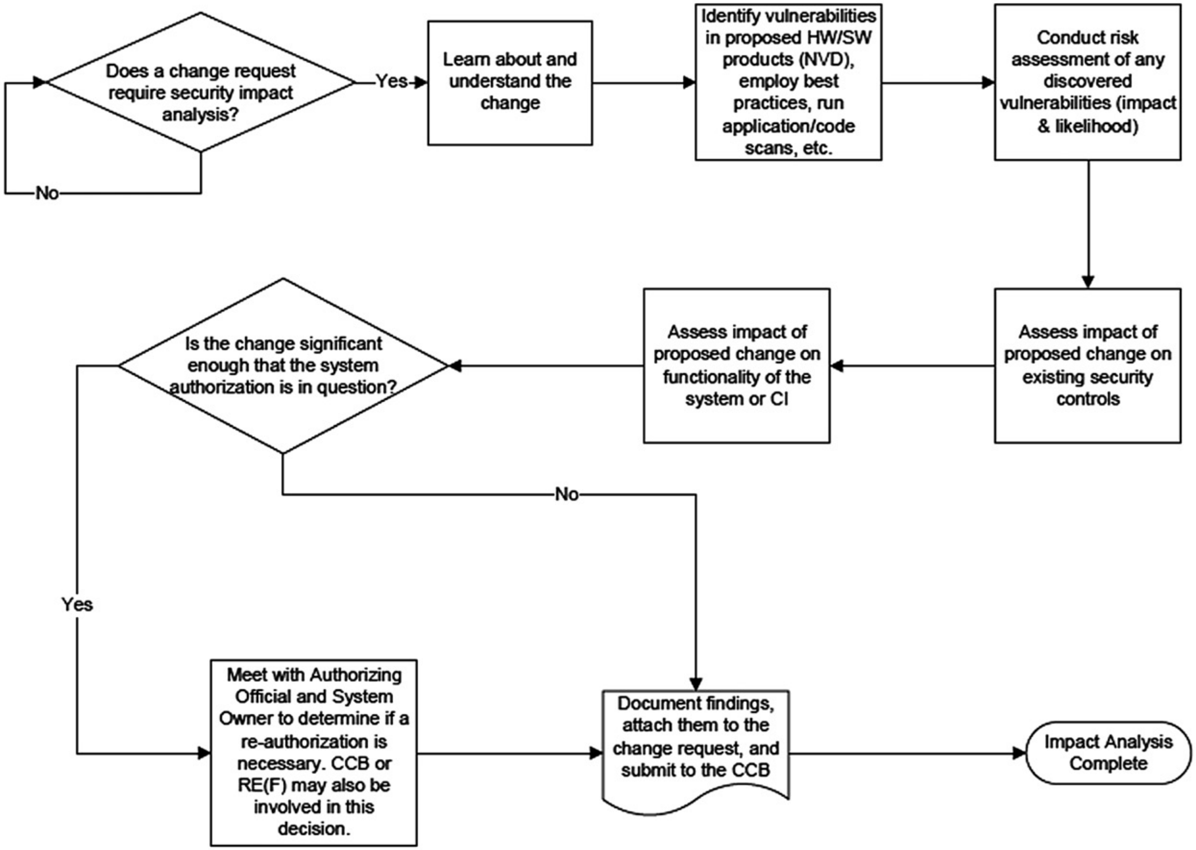

Does a change request require security impact analysis?
Yes
No
Learn about and understand the change
Identify vulnerabilities in proposed HW/SW products (NVD), employ best practices, run application/code scans, etc.
Conduct risk assessment of any discovered vulnerabilities (impact & likelihood)
Assess impact of proposed change on existing security controls
Assess impact of proposed change on functionality of the system or CI
Is the change significant enough that the system authorization is in question?
No
Yes
Meet with Authorizing Official and System Owner to determine if a re-authorization is necessary. CCB or RE(F) may also be involved in this decision.
Document findings, attach them to the change request, and submit to the CCB
Impact Analysis Complete

FIGURE 5.14 Configuration Management and Control Flow—Security Impact Analyses [16]

effects of frequent changes in hardware, software, and/or firmware components of an information system would, therefore, likely be controls with higher volatility" [3].

The continuous assessments of security controls identified for ongoing monitoring could produce weaknesses or deficiencies in addition to those discovered during the initial security authorization process. These corrective actions (and recommendations) will follow a similar strategy for risk mitigation[139] planning discussed in the NIST RMF (*Step 5*), including updates in the POA&Ms.[140]

Key Updates and Status Reporting

During continuous monitoring, results of security control assessments modifications to security control implementations, or changes to the information system may require updates to key documents in the authorization package.[141] Figure 5.12 provides recommendations on when potential updates may be required for each document to support the ongoing authorization of the information system or to facilitate near real-time risk management.

On an ongoing basis, results of the continuous monitoring activities are reported to the authorizing official by the system owner (or common controls provider). The frequency of updates through security status reports may be based on the monitoring strategy, and could occur more frequently when significant changes occur to the information system or significant deficiencies[142] (or material weaknesses) are identified (see Table 5.12).

[139] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process."*

[140] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Security controls that are modified, enhanced, or added during the continuous monitoring process are reassessed by the assessor to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk."*

[141] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The documents in the authorization package are considered 'living documents' and updated accordingly based on actual events that may affect the security state of the information system."*

[142] From Lew, J. Office of Management and Budget (OMB) Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. Washington: Executive Office of the President, Office of Management and Budget; 2011. *"A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets."*

Table 5.12 Key Document Updates

Key Document	Definition [3]	Owner	When to Update?
Security Plan	• An overview of the security requirements; describes the security controls in place or planned for meeting those requirements • Information to understand the intended or actual implementation of each security control employed within or inherited by the information system • Supporting appendices or, as references to appropriate sources, other risk-and security-related documents such as a • risk assessment; • privacy impact assessment (PIA); • system interconnection agreements; • contingency plan; • security configurations; • configuration management plan; • incident response plan; and • continuous monitoring strategy	Information system owner or common control provider	Whenever events[a] dictate changes (or modifications) to security controls
Security Assessment Report (SAR)	• A list of recommended corrective actions for any weaknesses or deficiencies identified in the security controls	Security control assessor	Whenever changes[b] are made to security controls (and additional assessment activities are performed)

Table 5.12 Key Document Updates (*continued*)

Key Document	Definition [3]	Owner	When to Update?
Plan of Action and Milestones (POA&Ms)	• Describes the specific measures planned: (i) to correct weaknesses or deficiencies noted in the security controls during the assessment; and (ii) to address known vulnerabilities in the information system • Content and structure of plans of action and milestones are informed by the organizational risk management strategy developed as part of the risk executive (function) and is consistent with the plans of action and milestones process established by the organization and any specific requirements defined in federal policies, directives, memoranda, or regulations	Information system owner or common control provider	At least quarterly,[c] whenever changes occur to the POA&M status such as progress made, and to address vulnerabilitie discovered during security impact analyses or continuous monitoring

[a] *From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. "Updates to the security plan may be triggered by a variety of events, including for example: (i) a vulnerability scan of the information system or vulnerability assessment of the environment of operation; (ii) new threat information; (iii) weaknesses or deficiencies discovered in currently deployed security controls after an information system breach; (iv) a redefinition of mission priorities or business objectives invalidating the results of the previous security categorization process; and (v) a change in the information system (e.g. adding new hardware, software, or firmware; establishing new connections) or its environment of operation (e.g. moving to a new facility)."*

[b] *From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. "Updates to the security assessment report help to ensure that the information system owner, common control provider, and authorizing officials maintain the appropriate awareness with regard to security control effectiveness."*

[c] *From Bolten, J. Office of Management and Budget (OMB) Memorandum 04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act. Washington: Executive Office of the President, Office of Management and Budget; 2004. Program officials shall regularly (at least quarterly and at the direction of the CIO) update the agency CIO on their progress to enable the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB [per FY2011 FAQ on FISMA Reporting (M-11-33) — "No FISMA submissions will be accepted outside of CyberScope"].*

Ongoing Risk Determination and Acceptance

The status update reports by the system owner (or common controls provider) are reviewed by the authorizing official on an ongoing basis. The status reports are coordinated with the organization's senior information security officer and the risk executive that provide input to the authorizing official in determining if the risk to the information system continues to be acceptable. The use of automated tools can assist in capturing, maintaining, and presenting (i.e., quantifying and visually displaying) security status information to support "near real-time" risk management, by communicating the overall risk posture. If automation is not available, a summary of the key changes to the documents included in the authorization package should be used by the authorizing official to understand and determine if changes would affect the original authorization decision (i.e., affects on the mission or business) for using and operating the information system.

SUMMARY

In this chapter, FISMA was introduced as a basis for understanding the key requirements for federal information security programs, including the roles and responsibilities for managing information security risks. The implementation of FISMA requires the application of organization-wide risk management activity. The management of risk is a complex and multifaceted activity requiring risks to be addressed at the strategic and tactical levels, and through different viewpoints. Integrating risk management into the organization's SDLC will result in the consistent application of risk management processes and procedures. Although this chapter limited the discussion of risk management process and decision making at the organizational level (which will be covered in the next chapter), the NIST RMF and related risk management and security tasks were covered in detail for managing risks from an information system perspective.

References

[1] Bolten J. Office of Management and Budget (OMB). FY 2003 report to Congress on federal government information security management. Washington: Office of Management and Budget; 2004.

[2] E-Government Act of 2002 [Internet]. Washington: US Government Printing Office [cited December 5, 2011]. <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm>.

[3] Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 revision 1, Guide for applying the risk management framework

to federal information systems: a security life cycle approach. Maryland: National Institute of Standards and Technology; 2010.

[4] Brown P, Kissel R. NIST Interagency Report (IR) 7358, Program review for information security management assistance. Maryland: National Institute of Standards and Technology; 2007.

[5] Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing information security risk: organization, mission, and information system view. Maryland: National Institute of Standards and Technology; 2011.

[6] Federal Chief Information Officers Council. Federal enterprise architecture security and privacy profile (FEA-SPP), version 3.0. Washington: Office of Management and Budget; 2011.

[7] Evans D, Bond P, Bement A. FIPS, 199 standards for security categorization of federal information and information systems. Maryland: National Institute of Standards and Technology; 2004.

[8] Stine K, Kissel R, Barker W, Fahlsing J, Gulick J. NIST Special Publication (SP) 800-60 Revision 1, Volume I: Guide for mapping types of information and information systems to security categories. Maryland: National Institute of Standards and Technology; 2008.

[9] E-Government Task Force. E-Government Strategy. Washington: Executive Office of the President, Office of Management and Budget; 2002.

[10] Federal Enterprise Architecture Program Management Office (FEAPMO). Business reference model (BRM) version 1.0. Washington: Executive Office of the President, Office of Management and Budget; 2002.

[11] Federal Enterprise Architecture Program Management Office (FEAPMO). Consolidated reference model version 2.3. Washington: Executive Office of the President, Office of Management and Budget; 2007.

[12] Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 3, Recommended security controls for federal information system and organizations. Maryland: National Institute of Standards and Technology; 2010.

[13] Gutierrez C, Jeffrey W. FIPS 200, Minimum security requirements for federal information and information systems. Maryland: National Institute of Standards and Technology; 2006.

[14] FedRAMP PMO. FedRAMP FAQ [Internet]. Washington: US General Services Administration [cited December 20, 2011]. <http://www.gsa.gov/portal/category/102439#12>.

[15] Ross R. FISMA Implementation project [Internet]. Maryland: National Institute of Standards and Technology [cited December 21, 2011]. <www.nasa.gov/ppt/482348main_2010_Monday_2_ross.ppt>.

[16] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D. NIST Special Publication (SP) 800-128, Guide for security-focused configuration management of information system. Maryland: National Institute of Standards and Technology; 2011.

[17] Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53A Revision 1, Recommended security controls for federal information system and organizations. Maryland: National Institute of Standards and Technology; 2010.

[18] Daniels M. Office of Management and Budget (OMB). Memorandum 02-01, Guidance for preparing and submitting security plans of action and milestones. Washington: Executive Office of the President, Office of Management and Budget; 2001.

[19] Federal Enterprise Architecture Program Management Office (FEAPMO). FEA practice guidance. Washington: Executive Office of the President, Office of Management and Budget; 2006.

[20] Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and privacy controls for federal information system and organizations. Maryland: National Institute of Standards and Technology; 2012.

[21] FedRAMP Program Management Office (PMO). FedRAMP FAQ [Internet]. Washington: US General Services Administration [cited December 20, 2011]. Available from: http://www.gsa.gov/portal/category/102439#12.

[22] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for applying the risk management framework to federal information systems: a security life cycle approach. Maryland: National Institute of Standards and Technology; 2010. *"The security assessment report provides visibility into specific weaknesses and deficiencies in the security controls employed within or inherited by the information system that could not reasonably be resolved during system development."*

This page is intentionally left blank

CHAPTER

Risk Management

6

INFORMATION IN THIS CHAPTER:

- Introduction to Risk Management
- Federal Information Security Risk Management Practices
- Overview of Enterprise-Wide Risk Management
- NIST Risk Management Process
- Comparing the NIST and ISO/IEC Risk Management Processes

INTRODUCTION TO RISK MANAGEMENT

The role of risk management within the federal government has evolved from focusing primarily on the assessment of risk[1] associated within a single information system[2] to an integration of risk-related activities that involves all levels[3] of the organization.[4]

[1] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments. Maryland: National Institute of Standards and Technology; 2011. *"Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence."*

[2] From Sterne, D., Balenson, D., Branstad, M., Jaworski, L., Lee, M.P., Pfleeger, C., at el. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook. Maryland: National Institute of Standards and Technology; 1995. *"Risk management is made up of two primary and one underlying activities; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one."*

[3] From Joint Task Force Transformation Initiative Interagency Working Group. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *The integration of risk management as an organizational function focuses on a three-tiered approach: organization level (tier 1); mission/business process level (tier 2); and information system level (tier 3).*

[4] From Joint Task Force Transformation Initiative Interagency Working Group. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *Risk management is "the program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time."*

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00006-X

By recognizing that organizations[5] are operating in highly complex, interconnected environments using state-of-the-art and legacy information systems [1], the application of the risk management process becomes more important to ensure the responsibility for information security risk management exists as an organization-wide activity. This organization-wide activity extends from those responsible for the strategic planning to those that operate the information systems in support of the mission and business operations. In Chapter 5, risk management was discussed from the perspective of the information system through the NIST Risk Management Framework (RMF)[6] to integrate risk management activities into the NIST system development lifecycle (SDLC).[7] Risk management in this chapter will examine risk management from a broader perspective. By discussing risk management as a holistic process which can include multiple perspectives (i.e., *organization*, *mission and business process*, and *information system*), we can obtain an understanding of how it would be applied across the entire organization or across multiple organizations.

Enterprise Risk Management (ERM)[8] is facilitated through the organization's risk management processes[9] to ensure the management of risk is applied consistently

[5] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *The term organization describes an entity of any size, complexity, or positioning within an organizational structure (e.g. a federal agency or, as appropriate, any of its operational elements) that is charged with carrying out assigned mission/business processes and that uses information systems in support of those processes.*

[6] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *The Risk Management Framework (RMF) provides a structured process that integrates risk management activities into the system development life cycle. The RMF operates primarily at tier 3 but also interacts with tier 1 and tier 2 (e.g. providing feedback from authorization decisions to the risk executive (function), disseminating updated risk information to authorizing officials, common control providers, and information system owners).*

[7] The NIST SDLC process includes five phases: *initiation, development/acquisition, implementation, operation/maintenance,* and *disposal.*

[8] From Flaherty, J., Rittenberg, L., Anderson, A., Jessup, J., Cyprus, N., Minter, F., et al. Enterprise Risk Management—Integrated Framework: Executive Summary. Washington, DC: Committee of Sponsoring Organizations of the Treadway Commission; 2011. *"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

[9] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. "*The NIST risk management process is complementary to and should be used as part of a more comprehensive Enterprise Risk Management (ERM) program.*"

across the enterprise. An ERM program is integrated across the organization through a comprehensive set of processes and practices that focus on managing organizational risk.[10] For risk management to be effective in managing security risks, it is essential that those with the responsibility for executing the mission and business operations have a clear understanding of their associated roles and responsibilities within the information security program.

An effective risk management program is driven from a "top-down" approach where the commitment and support for the program is enabled through the prioritization and allocation of resources needed for the program. In addition to resourcing risk management, the risk management strategy needs to be developed and communicated by the organization's senior management to ensure the risk management processes and practices are supported by the governance structure which links information system security risks to organizational impacts.[11] The organization's senior management/executives play a critical role to ensure information security risks are considered from an organizational perspective. Their role includes [1]:

- Assigning risk management responsibilities;
- Recognition and understanding that management of information security risks is an ongoing activity;
- Establishing and communicating the risk tolerance[12] throughout the organization; and
- Ensuring accountability for risk management decisions and effective, organization-wide risk management programs.

[10] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Organizational risk can include many types of risk (e.g. program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk)."*

[11] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Information systems are subject to serious threats that can have adverse effects on organizational operations (i.e. missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems."*

[12] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *Risk tolerance is the level of risk or degree of uncertainty that is acceptable to organizations and is a key element of the organizational risk frame.*

FEDERAL INFORMATION SECURITY RISK MANAGEMENT PRACTICES

Risk management is not a new concept within the federal government. As early as 1974, guidelines have been developed to support federal agencies in integrating risk management practices into federal security programs. For example, the National Bureau of Standards (NBS)[13] published the *Guidelines for Automatic Data Processing Physical Security and Risk Management* for the purpose of assisting automatic data processing (ADP) facility managers in developing physical security programs. These guidelines provided procedures for risk management–related activities such as conducting a risk analysis (*risk assessment*) and the selection and implementation of security measures (*risk mitigation*). This early risk management philosophy became the foundations by which federal information security programs were built.[14] As chronicled in Table 6.1, over the years, the federal government's viewpoint on risk management has changed, requiring the practices to evolve from a tactical to a strategic focus.

Risk management practices are a critical part of federal information security that require addressing continuous changes in the sophistication and complexity of the threat environment. In the past, federal agencies have been required to rely upon only risk assessments as a tool for integrating risk management activities within their certification and accreditation (C&A)[15] processes [9] and as the foundation[16] for managing risks within their information security programs. However, federal risk management processes are maturing. By adopting a government-wide approach, federal risk management programs are becoming more comprehensive through the use of continuous monitoring tools and techniques to gather security-related information to manage risks. Therefore, throughout the remainder of this chapter, the focus will shift to discussing a holistic, enterprise perspective to managing risk and the role of risk management in supporting a government-wide approach to security assessment, authorization, and continuous monitoring.

[13] NBS became the National Institute of Standards and Technology (NIST) in 1988.

[14] From Stoneburner, G., Goguen, A., Feringa, A. NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems. Maryland: National Institute of Standards and Technology; 2002. *"Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment."*

[15] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *The Joint Task Force Transformation Initiative Working Group transformed the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF).*

[16] From Crumpacker, J. Information Security Risk Assessment, Practices of Leading Organizations. Washington: US Government Accountability Office; 1999. *Risk assessments provide the foundation for other elements of the risk management cycle through which appropriate policies are developed and cost-effective techniques to implement these policies are selected.*

Table 6.1 Chronology of Federal Information Security Risk Management References

Date	Title and Description	Author
June 1974	*Guidelines for Automatic Data Processing Physical Security and Risk Management* provided “a handbook for use by Federal organizations in structuring physical security and risk management programs for their ADP facilities” [2].	NBS
May 1975	*Computer Security Guidelines for Implementing the Privacy Act of 1974* provided “a handbook for use by Federal organizations in implementing any computer safeguards which they must adopt in order to implement the Act” [3]. It included conducting Security Risk Assessments.	NBS
August 1979	*Guidelines for Automatic Data Processing Risk Analysis* provided the first formal set of guidelines for federal agencies when performing a risk analysis.	NBS
October 1989	*Guide for Selecting Automated Risk Analysis Tools* “assisted managers in selecting the most appropriate risk analysis tool” [4]. Although excluding specific focus on conducting risks analyses, it did cover the elements[a] of risk analysis for the purpose of selecting a tool.	National Institute of Standards and Technology (NIST)
January 1991	*Computers at Risk*[b] recommended the development of Generally Accepted System Security Principles (GASSP).	National Research Council (NRC) of the National Academies of Science (NAS)
October 1992	*A Framework for Computer Security Risk Management* provided a computer security risk management framework developed in collaboration among NIST/NSA, other countries, and the private sector.	Dr. Stuart Karzke (NIST)
October 1995	*An Introduction to Computer Security: The NIST Handbook* provided “assistance in securing computer-based resources by explaining important concepts, cost consideration and interrelationships of security controls” [12]. In addition, it included a chapter focused specifically on risk management.	NIST
September 1996	*Generally Accepted Principles and Practices for Securing Information Technology Systems* which provided security principles (used by individuals responsible for security at the system and organizational level) and practices[c] to be applied in the use, protection, and design of government information and data systems [5]. *The NIST Handbook* is a companion reference that was used as the basis for identifying common practices that support building an IT security program.	US GAO

Table 6.1 Chronology of Federal Information Security Risk Management References (*continued*)

Date	Title and Description	Author
May 1998	*Information Security Management, Learning From Leading Organizations* highlighted five management principles that were implemented by leading private sector organizations: assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. These principles aligned with the embodied framework established by the Federal Information Security Management Act (FISMA).	US GAO
November 1999	*Information Security Risk Assessment, Practices of Leading Organizations* was published to "identify and describe (1) information security risk assessment methods and (2) related critical success factors that could be considered by federal agencies to improve their own processes" [6].	US GAO
November 2000	*Federal Information Technology Security Assessment Framework* provided a method for agency officials when assessing status of their security programs and identify improvements.	NIST
July 2002	*Risk Management Guide for Information Technology Systems* provided a foundation for developing a risk management program.	NIST
March 2011	*Managing Information Security Risk: Organization, Mission, and Information System View* provided guidance for managing information security risk with specific details of assessing, responding to, and monitoring risk on an ongoing basis [7].	NIST
September 2011	*Guide for Conducting Risk Assessments* refocused from the previous publication to address risk assessments as part of the risk management framework [8].	NIST

[a] *Asset identification, threat assessment, vulnerability assessment, and safeguard effectiveness.*

[b] *"Computers at Risk: Safe Computing in the Information Age," National Academy Press (1991), was a report of the System Security Study Committee (formed in 1990 by the Computer Science and Telecommunications Board). Available from: http://www.nap.edu/catalog.php?record_id=1581.*

[c] *NIST used the Organization for Economic Co-Operation and Development's (OECD) "Guidelines for the Security of Information Systems" when developing the principles for federal information systems. The OECD document was updated in 2002 and renamed from the original publication in 1992 to "OECD Guidelines for the Security of Information System and Networks."*

OVERVIEW OF ENTERPRISE-WIDE RISK MANAGEMENT

Enterprise-wide risk management consists of a structured approach for consistently and continuously applying risk management practices for managing risk[17] beyond the information system boundary. By examining the components that make up the federal government's viewpoint of an organization-wide risk management program, a model can be established that will be useful for integrating these components into existing federal government and private sector risk management programs. As previously discussed, risk management within the federal government has primarily focused on managing risk at the information system level. This system level approach is not adequate when risks need to be communicated across the different levels of the organization or between multiple organizations. For risk management to be effective as a strategic and tactical tool used by the organization(s) in making risk decisions, it needs to be able to manage risk across the complex environments in which information systems operate. In this section, an overview will be provided of the integrated, enterprise-wide risk management[18] methodology, and how it is applied in the context of the organization(s)[19] supported by the information system. In addition, to provide a broader context, the next section will include a brief comparison of both the practices and processes used in the federal government and in the private sector using international risk management standards.

Components of the NIST Risk Management Process

The risk management process (or cycle)[20] consists of four components that provide a structured, process-oriented approach for managing risks. Each of the four

[17] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. "*Risk refers to information security risk from the operation and use of organizational information systems including the processes, procedures, and structures within organizations that influence or affect the design, development, implementation, and ongoing operation of those systems*."

[18] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Integrated, enterprise-wide risk management includes, for example, consideration of: (i) the strategic goals/objectives of organizations; (ii) organizational missions/business functions prioritized as needed; (iii) mission/business processes; (iv) enterprise and information security architectures; and (v) system development life cycle processes."*

[19] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Any entity of any size, complexity, or positioning with an organizational structure that is charged with carrying out assigned mission/business processes and that uses information system in support of those processes."*

[20] From Office of Electricity Delivery & Energy Reliability. Electricity Sector Cybersecurity Risk Management Process Guideline. Washington: US Department of Energy. "*The risk management cycle is a comprehensive process that requires organizations to (1) frame risk (i.e., establish the context for risk-based decisions), (2) assess risk, (3) respond to risk once determined, and (4) monitor risk on an ongoing basis, using effective organizational communications and an iterative feedback loop for continuous improvement in the risk-related activities of organizations*."

components of the risk management process ensures risk is managed in an integrated process that requires the involvement of the entire organization. Historically, the federal government included only two of the four components of risk management—*risk assessment* and *risk response*. In this approach to risk management, as illustrated in Figure 6.1, two additional components have been added: *risk framing* and *risk monitoring*.

Risk Framing

Establishing a risk context (or framing) is a critical first step in risk management that requires describing the risk environment, including any boundaries for making risk-based decisions. The environment includes risk assumptions,[21] risk constraints,[22] risk tolerance,[23] priorities/trade-offs,[24] and the trust model.[25] Framing the risk can also include information about any tools or techniques that are used by the organization to support the risk management activities. The output of risk framing is a risk management strategy[26] which provides the organization with a common perspective for managing risks (i.e., assessment, response, or monitoring).

[21] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. "*Assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time*."

[22] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. "*Constraints on the risk assessment, response, and monitoring alternatives under consideration*."

[23] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. "*Levels of risk, types of risk, and degree of risk uncertainty that are acceptable*."

[24] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. "*The relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses*."

[25] Trust models can be formed through evidence-based assurance (*validated trust*), historical relationships (*direct historical trust*), third-party assurance (*mediated trust*), authoritative organizations (*mandate trust*), or any combination (*hybrid trust*) of the previous trust models for one organization to obtain the necessary level of trust of the security/risk activities of another organization.

[26] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *A risk management strategy "addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions."*

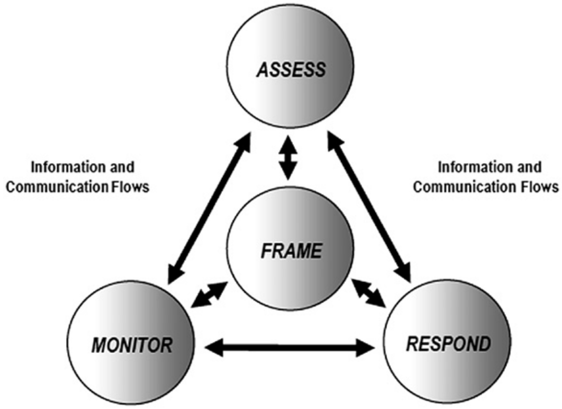

ASSESS
Information and Communication Flows
Information and Communication Flows
FRAME
MONITOR
RESPOND

FIGURE 6.1 Components of the Risk Management Process

Risk Assessment

The assessment of risk is based on the organization's risk context, and includes activities focused on supporting the identification and determination of risk, and monitoring risk factors.[27] Risks are identified based on a characterization of threats[28] (threat sources and events), vulnerabilities[29] and predisposing conditions.[30] The risk determination is based on the impact that would result from an event and the likelihood the event would occur. Monitoring risk factors is the maintenance aspect, and includes

[27] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments. Maryland: National Institute of Standards and Technology; 2011. *Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments and can include threat information, vulnerabilities, and preconditions.*

[28] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments. Maryland: National Institute of Standards and Technology; 2011. *"An event or situation that has the potential for causing undesirable consequences or impact."*

[29] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments. Maryland: National Institute of Standards and Technology; 2011. *"Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."*

[30] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments. Maryland: National Institute of Standards and Technology; 2011. *"A condition that exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operation, which affects (i.e. increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation."*

an ongoing situational awareness of the changes to information used by the organization when making a risk-based decision.

A risk assessment is a tool that can be used organization wide. Depending on the organizational structure, risk-related information captured at the strategic level (*tier 1*), as illustrated in Figure 6.2, can be used at the tactical level (*tier 3*). By conducting risk assessments as a continual risk management activity, threats, vulnerability, likelihood, and impact information can be refined and updated with information at each of the three levels within the organization (*governance*, *mission/business process*, and *information system*). However, to effectively integrate risk assessments at the different levels within the organization, the involvement in the risk assessment activities must extend beyond those responsible for information security. By using an organizational approach to conduct risk assessments, information security risks become an integral part of the organization's overall decision-making process.

Risk Response

After risks have been identified and analyzed, the organization focuses on developing responses[31] to risk. When responding to risks, the organization needs to ensure the response is consistent with the risk context defined in the risk framing component of risk management. Depending on the level of the organization, the risk response may be different due to the types of risk-related information being evaluated for impact and the specific interpretation of the risk management strategy. For example:

- The focus of risk response at the strategic, organizational level might focus on the actions (e.g., accept risk, avoid risk, and transfer risk) that would be available to the organization based on the risk framing.
- Risk responses from the perspective of the mission/business process owners might consider impacts on the ability of the specific organization to accomplish a specific business function which could result in changes to the information security architecture or processes that support the information security program.
- Risk response at the tactical, information system level might focus on specific tasks (plans of action and milestones) that would be undertaken to correct any weaknesses or deficiencies found in security controls to ensure risk is mitigated to an acceptable level.

A key part of risk response that cannot be overlooked is how the responses to risk are communicated outside of the organization such as with external service providers (or

[31] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"The purpose of the risk response component is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action."*

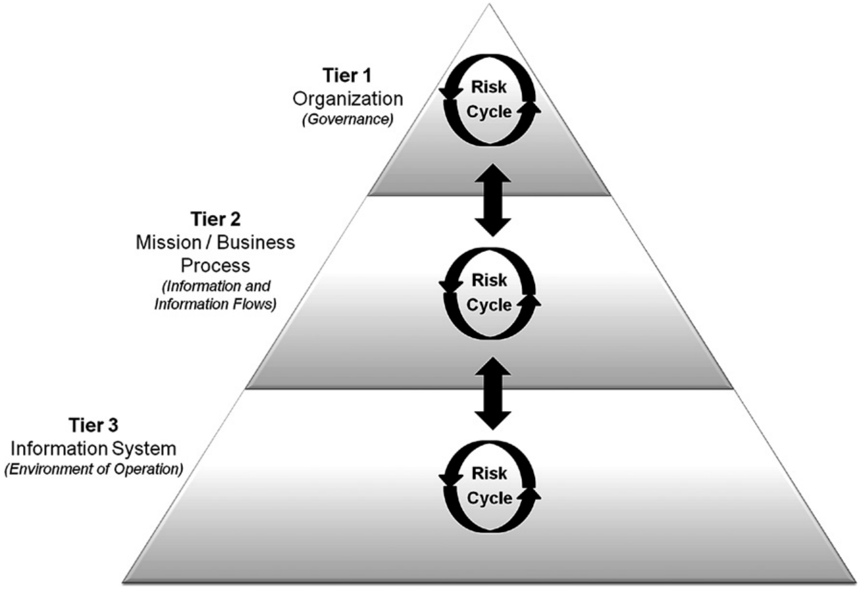


FIGURE 6.2 Multi-Tiered Integration of the Risk Management Process

even between organizations) who may share some or all of the risks. This may require those service providers (or organizations) to be part of the risk response decision-making process, specifically if it relates to contractual or service-level obligations that have already been established and formalized prior to the risk response decisions.

Risk Monitoring

The purpose of risk monitoring is to address how risk will be monitored. This includes verifying compliance with the risk response decisions by ensuring the organization implements the risk response measures (and any information security requirements), determines the ongoing effectiveness of risk response measures, and identifies any changes that would impact the risk posture [1]. Risk monitoring activities at the various levels of the organization (or with other organizational entities) should be coordinated and communicated. This can include sharing risk assessment results that would have an organization-wide impact to risk responses being planned or implemented. The organization should also consider the tools and technologies that will be needed to facilitate monitoring and the frequency necessary for effectively monitoring risks, including the changes that would impact responses to risks.

Multi-Tiered Risk Management

Most organizations, regardless of the size or type, have a similar structure that includes executive leadership (addressing risk as it relates to the organization's mission and

NOTE

Five potential outcomes of the governance-related risk management activities [1] include:

- Strategic alignment of risk management decisions consistent with the organization's goals and objectives.
- Execution of risk management processes (i.e., frame, assess, respond to, and monitor).
- Effective and efficient allocation of risk management resources.
- Performance-based outcomes (e.g., risk management metrics) that ensure organizational goals and objectives are being achieved.
- Optimizing risk management investments to support organizational objectives.

business functions), mission and business management (addressing risk as it relates to the organization's operations), and system management (addressing risk as it relates to the security controls). As illustrated in Figure 6.2, the integration of the risk management process focuses on the risk management activities[32] at each tier.

The information flow between the organizational tiers should be bi-directional. By offering a feedback loop, results of monitoring activities can be shared between organizational tiers at each level within the governance structure (or model[33]). For example, *tier 3* outputs can be used by *tier 2* to improve policies, procedures, and practices, and *tier 2* outputs can be used to by *tier 1* to improve organizational policies that govern the risk management program and are articulated through the risk management strategy. Not only is the information flow important for the facilitation of internal risk-related information, it can also serve to communicate information from external sources (e.g., peer organizations, service providers) that may improve the strategy to ensure it is comprehensive.

Tier 1 Risk Management Activities

The organization's governance[34] structure and practices are generally developed from a "top-down" approach. This ensures the organizational governance (i.e., responsibilities and practices) addresses risk from an organizational viewpoint that is consistent with the strategic goals and objectives. In addition, risk management process should be directed from the senior management (head of a federal agency, corporate executive, etc.) to align the risk decision with the organization's strategic direction. Senior management may also have the overall responsibility for overseeing the achievement of the business objectives and thus they may have the ability to ensure resources are available and used effectively to manage risk.

[32] Activities related to framing risk, assessing risk, responding to risk, and monitoring risk executed at each tier within the context of the organization's governance structure and risk management program.

[33] There are three basic types of security governance models: *centralized, decentralized,* and *hybrid.*

[34] Applying a consistent and unified governance approach facilitates cost-savings when applying risk management activities and translating risks between business functions.

In *tier 1*, the risk executive (or function) also plays an important role in supporting the risk management in determining how decisions made regarding risk are carried through the organization governance.[35]

Tier 2 Risk Management Activities

At *tier 2*, the business/mission processes[36] manage risk based on the components defined in the risk management strategy. Since these processes support the mission/business functions, they must have an awareness of impact. As an example, if a sophisticated cyber attack occurred, the mission/business processes need to be designed to achieve an anticipated level of resiliency. Therefore, a key consideration when defining the mission/business processes is the selection of a risk response strategy that is within the constraints defined in the risk management strategy[37] [1].

Tier 3 Risk Management Activities

The NIST SDLC integrates risk management activities through the application of the NIST RMF. The specific risk management activities at *tier 3* are guided by the output of the risk management activities conducted at *tier 1* and *tier 2*, (i.e., where the risk management strategy and the risk response strategy that is supported by an information security architecture).[38] In addition, the output of the risk management activities

[35] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *Risk management decisions include: (i) the types of that are reserved for specific senior management; (ii) the types that are deemed to be organization-wide and the types that can be delegated to subordinate organizations or to other roles in the organization; and (iii) how risk management decisions will be communicated.*

[36] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *A risk-aware mission/business process is one that explicitly takes into account the likely risk such a process would cause if implemented by and explicitly accounting for risk when evaluating the mission/business activities.*

[37] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *Risk response strategies specify the responsible parties, dependencies on other risk response strategies and other factors, implementation timeline, monitoring plans and triggers, and any temporary measures that can be implemented until the response strategy has been fully implemented.*

[38] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *The information security architecture represents that portion of the enterprise architecture specifically addressing information system resilience and providing architectural information for the implementation of security capabilities.*

TIP

Cloud computing is one example where trust and trustworthiness[39] between cloud service providers (CSPs) and a federal agency is critical for the effective application of the NIST RMF. The Federal Risk and Authorization Management Program (FedRAMP) "introduces an innovative policy approach to developing trusted relationships between Executive departments and agencies and cloud service providers (CSPs)" [10]. However, for a trusted relationship to exist, transparency into the risk management and information security activities must include operational visibility based on the adequate level of confidence needed by the federal agency using the cloud services. "Establishing a level of confidence about a cloud service environment depends on the ability of the cloud provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls"[13]. This might require documenting the risk information needed to address the trust requirements in contracts, service level agreements (SLAs), or other forms of legal agreements.

from the other tiers also ensures the information system operates consistently with the information system resiliency[40] requirements.

NIST RISK MANAGEMENT PROCESS

The risk management process can be applied as a tiered model as represented in Figure 6.3, in which each of the four risk management components, previously discussed, is applied at each tier. Each tier plays a role in the execution of the risk management process where information flows across the tiers bi-directionally. In this section each risk management process will be described and the specific interactions between the tiers will be highlighted. Although there is no specific order for applying the risk management processes within an organization, this section does address each process within each tier based on the presumption that a "top-down" approach will be used. The approach starts with *tier 1* where the risk framing step begins in the risk management cycle and concludes with monitoring risk before moving to the next tier (i.e., *tier 2* and *tier 3*).

[39] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *The attribute of a person or enterprise that provides confidence to others of the qualification, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.*

[40] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *Information system resiliency is the ability of an information system to continue to operate under adverse conditions and recover within a time frame consistent with the operational need.*

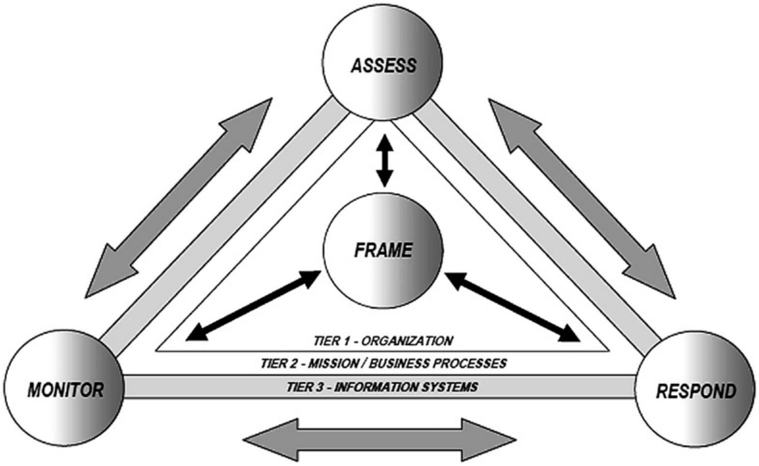

ASSESS
FRAME
MONITOR
RESPOND
TIER 1 - ORGANIZATION
TIER 2 - MISSION / BUSINESS PROCESSES
TIER 3 - INFORMATION SYSTEMS

FIGURE 6.3 Tiered Application of the Risk Management Process

Framing Risk

In the risk management process, risk framing establishes the risk management strategy which provides a common organization-wide strategy for executing the other steps (*assessment, response,* and *monitoring*) of the process that are supported by the commitment of the organizations, senior management. As illustrated in Figure 6.4, input to risk framing can include laws, policies, directives, regulations, contractual relationships, financial limitation's or information that explicitly (MOUs/MOAs, governance processes) supports key activities in the risk framing step.

Risk framing activities produce guidance that enables the development of a common perspective on how the organization manages risk. This perspective is established through the assumptions and constraints, level of risk tolerance, and priorities and trade-offs that drive the organizations' decision-making process, and the type/size of the organization. Since risk framing may initially be high level or undefined, a feedback loop should exist to ensure information from the other steps of the risk management process are used to adjust the original risk factors that contribute to the organization's risk management policies, procedures, standards, and guidance.

The risk framing step also produces the risk framework and risk methodologies[41] that will be used by the organization in *tier 2* and *tier 3* of the risk management hierarchy and in the execution of the other risk management steps. For example, if the

[41] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments. Maryland: National Institute of Standards and Technology; 2011. *A risk assessment methodology is a risk assessment process, together with a risk model, assessment approach, and analysis approach.*

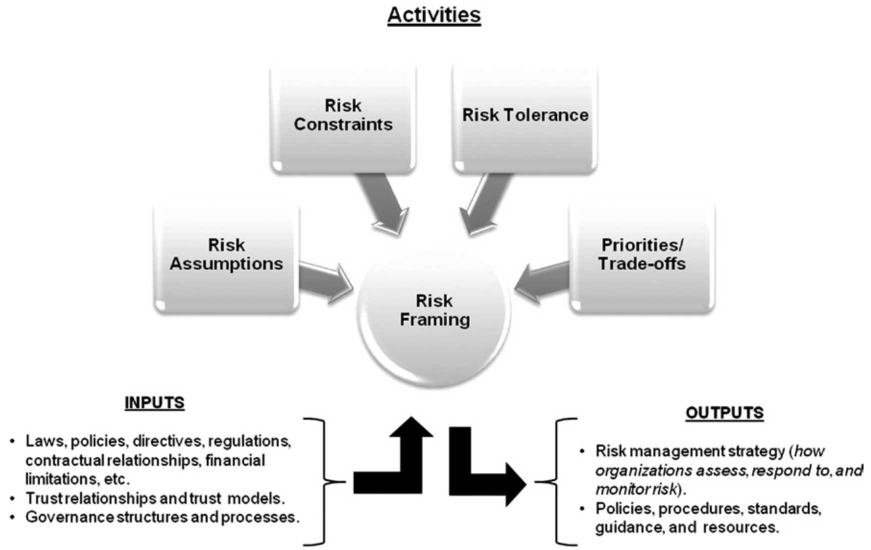

Activities
Risk Constraints
Risk Tolerance
Risk Assumptions
Priorities/ Trade-offs
Risk Framing
INPUTS
• Laws, policies, directives, regulations, contractual relationships, financial limitations, etc.
• Trust relationships and trust models.
• Governance structures and processes.
OUTPUTS
• Risk management strategy (how organizations assess, respond to, and monitor risk).
• Policies, procedures, standards, guidance, and resources.

FIGURE 6.4 Risk Framing—Inputs, Activities, and Outputs

organizational governance structure is centralized,[42] only one framework and methodology may be required, whereas if the organization is decentralized,[43] multiple frameworks and methodologies may be required. By having a common framework and methodology for organization-wide tailoring, it ensures at least there is a consistent evaluation standard used by the entire organization for assessing risk and prioritizing risks as they are aggregated (or consolidated) from across the organization. This standard can then be applied in the risk assessment step when assessing risks and in the risk response step when courses of action are prioritized and implemented to achieve the most cost-effective strategy for risk mitigation.[44]

[42] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *The authority, responsibility, and decision-making powers are vested solely within central bodies that establish the appropriate policies, procedures, and processes.*

[43] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *The authority, responsibility, and decision-making powers are vested in and delegated to individual subordinate organizations which establish their own policies, procedures, and processes.*

[44] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process."*

Risk Assessment

The risk assessment step of the risk management process, as shown in Figure 6.5, involves two major activities: *identifying threats and vulnerabilities* and *risk determination*. This step receives input from the other risk management processes to help the decision-makers at each level of the risk management hierarchy identify, prioritize, and estimate risks. The inputs to the risk assessment step include, for example, the risk assessment methodology (*risk framing*), different courses of actions (*risk response*), and new threats and vulnerabilities identified (*risk monitoring*).

Risk assessments can be a useful source of input for risk-related information when conducted at each of the organizational tiers. *Tier 1* and *tier 2* apply risk assessments based on information security related risks associated with organizational governance and management activities, mission/business processes (or enterprise architecture), and funding of information security programs [10]. *Tier 3* risk assessment activities focus primarily on support information system related activities conducted during the implementation of the NIST RMF as discussed in Chapter 5 (i.e., security categorization, security control selection, security control implementation, security control assessments, security authorization, and security control monitoring). Previously, risk assessments were only conducted at *tier 3* (information system level). Although, some risk information cannot be assessed effectively at *tier 3*, such as *tier 1* risks associated with the organization-wide security program or *tier 2* risks associated with common controls shared across the organization or between entities that have a trusted relationship.

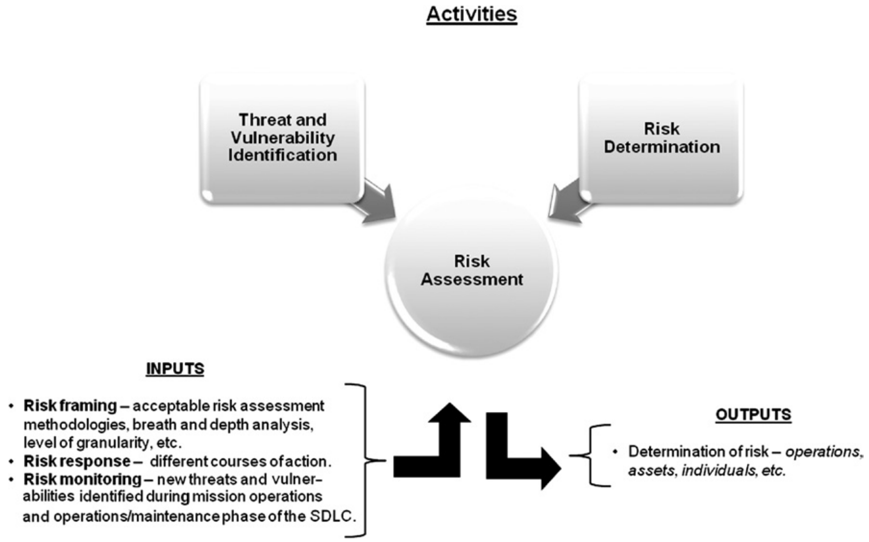

Activities
Threat and Vulnerability Identification
Risk Determination
Risk Assessment
INPUTS
• Risk framing – acceptable risk assessment methodologies, breath and depth analysis, level of granularity, etc.
• Risk response – different courses of action.
• Risk monitoring – new threats and vulnerabilities identified during mission operations and operations/maintenance phase of the SDLC.
OUTPUTS
• Determination of risk – operations, assets, individuals, etc.

FIGURE 6.5 Risk Assessment—Inputs, Activities, and Outputs

WARNING

According to NIST: *"... risk assessments are often not precise instruments of measurement and reflect:*

(i) the limitations of specific assessment methodologies, tools, and techniques employed;
(ii) the subjectivity, quality, and trustworthiness of the data used;
(iii) the interpretation of assessment results; and
(iv) the skills and expertise of those individuals or groups conducting the assessments.

Since cost, timeliness, and ease of use are a few of the many important factors in the application of risk assessments, organizations should attempt to reduce the complexity of risk assessments and maximize the reuse of assessment results by sharing risk-related information across their enterprises, whenever possible."

As previously noted, inputs to the risk assessment can come from a variety of sources. As illustrated in Figure 6.6, one of the most important sources is the organizational risk frame which establishes the context for the risk management strategy. The risk management strategy includes "information regarding policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, scope of the assessments, rigor of analyses, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the organization" [11]. The risk assessment methodology, a component of the risk management strategy, includes the definition of the risk assessment process, risk model (*risk factors and relationships among risk factors*), assessment approach (*quantitatively*,[45]*qualitatively*,[46] or *semi-quantitatively*[47]), and an analysis approach (*threat-oriented*, *asset/impact-oriented*, or *vulnerability-oriented*).

Responding to Risk

The risk response step in Figure 6.7 includes multiple activities for responding to risk such as identifying courses of actions, evaluating alternative courses of action, and selecting and implementing courses of action. As with risk assessment, the risk response is performed at each level of the risk management hierarchy, with activities performed at specific tiers. For example, risk response identification could require

[45] From Risk Steering Committee. DHS Risk Lexicon. Washington: US Department of Homeland Security; 2010. *"Set of methods, principles, or rules for assessing risk based on non-numerical categories or levels."*

[46] From Risk Steering Committee. DHS Risk Lexicon. Washington: US Department of Homeland Security; 2010. "Set of methods, principles, or rules for assessing risk based on non-numerical categories or le*vels."*

[47] From Risk Steering Committee. DHS Risk Lexicon. Washington: US Department of Homeland Security; 2010. *"Set of methods, principles, or rules to assess risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts."*

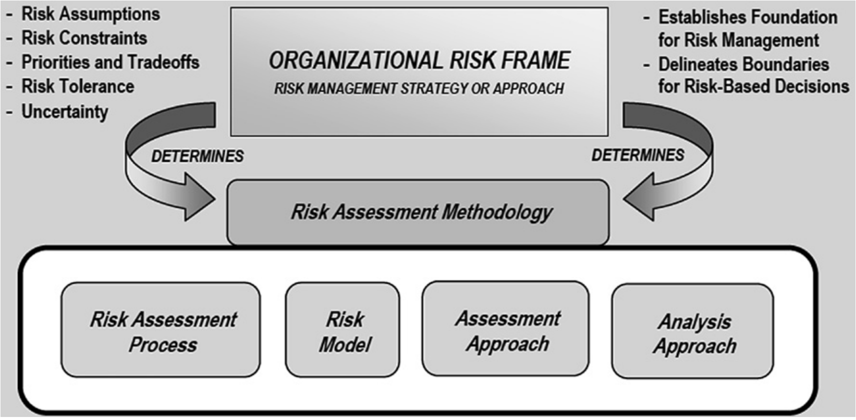

- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty
ORGANIZATIONAL RISK FRAME
RISK MANAGEMENT STRATEGY OR APPROACH
- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions
DETERMINES
DETERMINES
Risk Assessment Methodology
Risk Assessment Process
Risk Model
Assessment Approach
Analysis Approach

FIGURE 6.6 Components of a Risk Assessment [11]

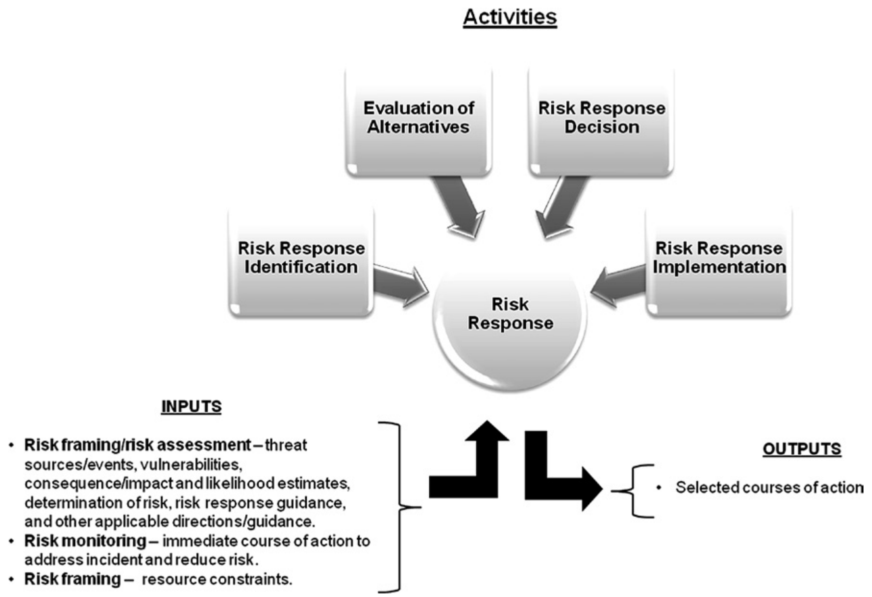

Activities
Evaluation of Alternatives
Risk Response Decision
Risk Response Identification
Risk Response Implementation
Risk Response
INPUTS
• Risk framing/risk assessment – threat sources/events, vulnerabilities, consequence/impact and likelihood estimates, determination of risk, risk response guidance, and other applicable directions/guidance.
• Risk monitoring – immediate course of action to address incident and reduce risk.
• Risk framing – resource constraints.
OUTPUTS
• Selected courses of action

FIGURE 6.7 Risk Response—Inputs, Activities, and Outputs

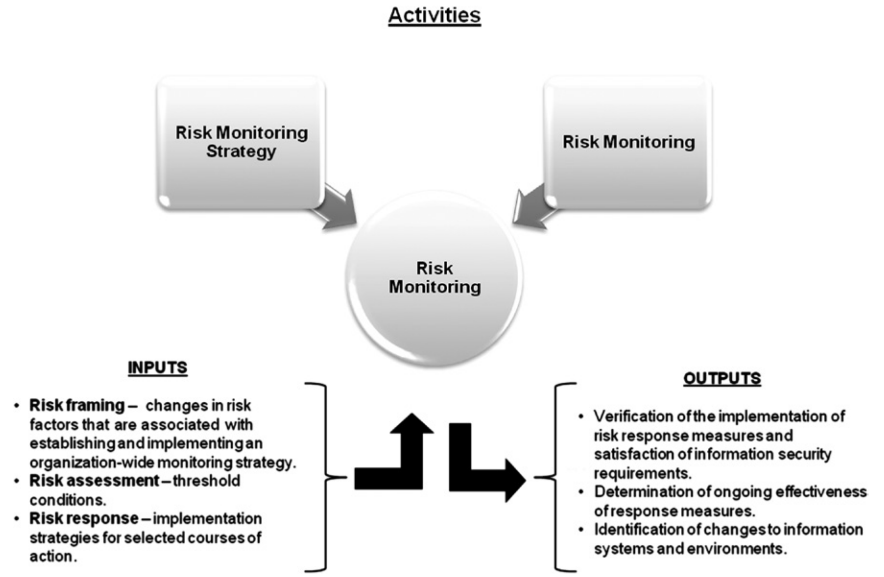

Activities
Risk Monitoring Strategy
Risk Monitoring
Risk Monitoring
INPUTS
• Risk framing – changes in risk factors that are associated with establishing and implementing an organization-wide monitoring strategy.
• Risk assessment – threshold conditions.
• Risk response – implementation strategies for selected courses of action.
OUTPUTS
• Verification of the implementation of risk response measures and satisfaction of information security requirements.
• Determination of ongoing effectiveness of response measures.
• Identification of changes to information systems and environments.

FIGURE 6.8 Risk Monitoring—Inputs, Activities, and Outputs

considering organization-wide impacts and therefore might be performed at *tier 1*, whereas evaluation of alternative courses of action could require an evaluation of impacts to mission/business processes and therefore might be performed at *tier 2*. Regardless at which tier the activity is performed, the risk decisions receive input from the other risk management processes that are shared and communicated.

Monitoring Risk

The last step in the risk management process involves monitoring risk. Figure 6.8 illustrates the two activities performed during the risk monitoring step: *risk monitoring strategy* and *risk monitoring*. Risk monitoring strategy includes defining the purpose of the risk monitoring program, type of monitoring to be performed (e.g., automated vs. manual) and frequency of monitoring activities. Risk monitoring provides organizations with the means to verify compliance,[48] determine the ongoing

[48] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Compliance verification ensures that organizations have implemented required risk response measures and that information security requirements derived from and traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines are satisfied."*

effectiveness of risk response measures[49] and identify risk-impacting changes to organizational information systems and environments of operation [1], which is driven by the monitoring strategy.

COMPARING THE NIST AND ISO/IEC RISK MANAGEMENT PROCESSES

Risk management methodologies[50] have been published by many organizations. In this section, a brief examination will be provided on the methodologies published by NIST and the International Organization for Standards /International Electrotechnical Commission (ISO/IEC). As a reference, Table 6.2 provides a list of risk management–related standards and guidelines published by NIST and the ISO/IEC, and can be useful as a basis for understanding how each approaches risk management.

Risk management practices are the foundation by which the risk management strategy is communicated through the governance structure. By understanding the general similarities and differences between each approach, it will enable federal agencies following the NIST methodology and private sector organizations following the ISO/IEC methodology to more consistently apply risk management practices across the organizational boundaries. As an example, Figure 6.9 provides a "high-level" comparison of the key processes included in the NIST and ISO/IEC risk management methodologies.

In *Step 1*, outlined in Table 6.3, both NIST and the ISO/IEC address framing the risk (or establishing the risk context).[51] In the NIST process, risk framing requires the organization to develop a risk management strategy that meets its unique governance structure, mission, and business operations. Although the NIST process

[49] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Effectiveness monitoring is employed by organizations to determine if implemented risk response measures have actually been effective in reducing identified risk to the desired level."*

[50] Examples include the Software Engineering Institute (SEI)'s *"Security Quality Requirements Engineering (SQUARE),"* available from: http://www.sei.cmu.edu/library/abstracts/reports/05tr009.cfm; the Software Engineering Institute (SEI)'s "*Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®),*" available from: http://www.cert.org/octave; the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s "*Enterprise Risk Management—Integrated Framework,*" available from: http://www.coso.org/erm-integratedframework.htm; and the Information Systems Audit and Control Association (ISACA)'s "*Risk IT,*" available from: http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx.

[51] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *Risk framing (or establishing context) includes defining the criteria used by organizations to determine* "*when risk assessment results do not warrant risk responses, then assessment results could be fed directly to the risk monitoring step as a source of input.*"

Table 6.2 NIST and ISO/IEC Risk Management Standards and Guidelines

ISO/IEC 27001:2005 Information technology—Security techniques—Information security management system—Requirements

ISO/IEC 27002:2005 Information technology—Security techniques—Code of practices for information security management

ISO/IEC 27005:2011[a] Information technology—Security techniques—Information security risk management

ISO/IEC 31000:2009 Risk management—Principles and guidelines

ISO/IEC 31010:2009 Risk management—Risk assessment techniques

NIST SP 800-30 Revision 1[b] Guide for Conducting Risk Assessments

NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations

NIST SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems and Organizations

NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View

[a]Replaced ISO/IEC 27005:2008 with the same name. [b]Replaced NIST SP 800-30 with a different title ("Risk Management Guide for Information Technology Systems").

Table 6.3 Key Process Activities—Step 1

NIST	ISO/IEC
• Development of the risk management strategy • Development of organizational policies, procedures, standards, guidance, and resources	• Setting basic criteria (approach, evaluation, impact, and acceptance) • Defining the scope and boundaries • Establishing an organization

presents a more flexible approach, it is limited in providing specific guidance for performing the risk framing activity, whereas the ISO/IEC process provides a more specific set of criteria to use when documenting the risk context.

TIP

NIST plays a critical role in aligning standards where possible with those developed internationally or nationally. Risk management is no exception. The goal of harmonization efforts performed by NIST is to limit "the burden on organizations that must conform to both ISO/IEC standards and NIST standards and guidance" [1].

In the next step, the NIST and the ISO/IEC processes include similar activities for supporting risk identification and risk determination activities. As shown in Table 6.4, both focus on the determination of risk through the identification of threats and vulnerabilities and the analysis of the risk-related information to support a risk determination. One specific difference is an additional activity in the ISO/IEC risk assessment process for evaluating risks to determine if any actions should be taken based on the output of risk analysis and risk prioritization. Additionally, both processes apply the context established in *Step 1* as an input into the assessment of risk within the risk management process.

In Table 6.5, the risk response (or risk treatment) options are selected for determining which courses of action (e.g., acceptance, avoidance, mitigation, etc.) to apply as a response to a particular risk. During the risk decision process in *Step 3*, both the NIST and the ISO/IEC recognize that regardless of the decision, there still remains a degree of residual risk that must be addressed and compared against the organization's risk tolerance [1]. However, as shown in Table 6.6, the ISO/IEC process (*Step 4*), includes an additional activity for the explicit and formal acceptance of residual risk.

Table 6.4 Key Process Activities—Step 2

NIST	ISO/IEC
• Identify threats and vulnerabilities • Determine risk	• Identify threat • Identify existing controls • Identify vulnerabilities • Identify consequences • Assess consequences • Assess incident likelihood • Determine risk level • Evaluate risks

Table 6.5 Key Process Activities—Step 3

NIST	ISO/IEC
• Identify risk responses • Evaluate response alternatives • Risk response decision • Risk response implementation	• Define a risk treatment plan • Modify risks based on changes in the controls selected

Table 6.6 Key Process Activities—Step 4

NIST	ISO/IEC
	• Accept information security risks

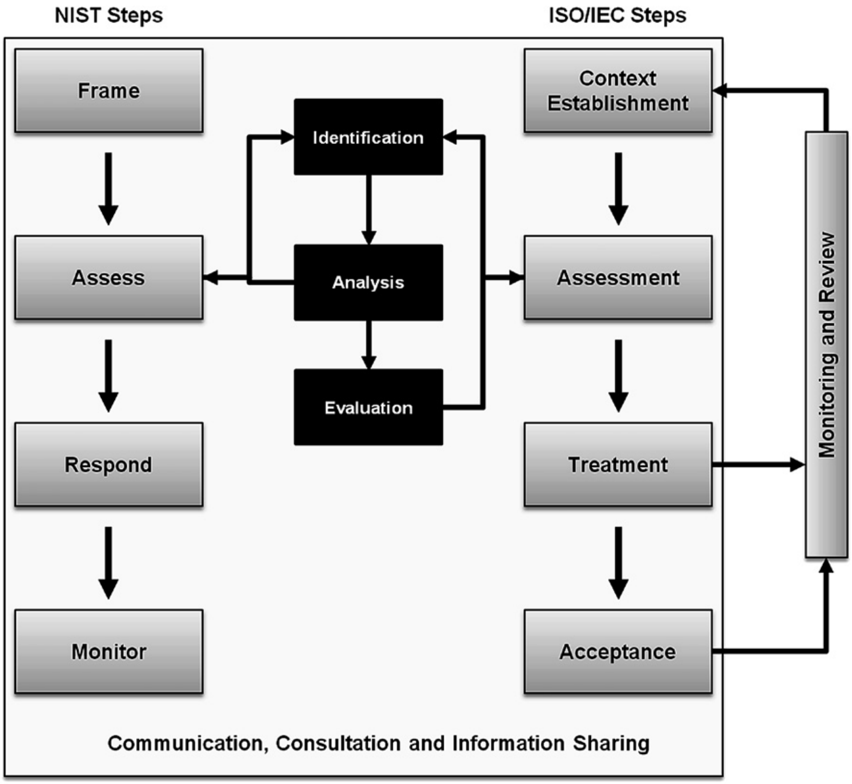


FIGURE 6.9 Comparison of Major NIST and ISO/IEC Risk Management Processes

The NIST process also includes risk acceptance, but as a separate course of action (i.e., acceptance of risk in the NIST RMF *Step 5* and *Step 6*) when responding to risk that has been determined to be within the organizational risk tolerance.

Both NIST and the ISO/IEC processes address the ongoing communications and sharing of risk-related information with decision makers and stakeholders impacted by the risk response decisions. This activity uses the bi-directional pathway to communicate risk information to ensure those with responsibility for implementing the risk decisions understand the actions that must be taken. Unlike the ISO/IEC process shown in Table 6.7, the NIST process does not specifically identify the communication, sharing, and exchanging of risk information as a separate step, rather it is linked to other risk management activities such as risk monitoring where risk-based decisions are made as an integral part of every tier within the organization's risk management hierarchy, i.e. *governance level, mission/business process level,* and *information system level*.

In the final step outlined in Table 6.8, monitoring (*Step 6*), both the NIST and the ISO/IEC processes focus on monitoring risks (and risk factors) for any changes.

Table 6.7 Key Process Activities—Step 5

NIST	ISO/IEC
	• Communicate, share, and exchange risk information

Table 6.8 Key Process Activities—Step 6

NIST	ISO/IEC
• Develop a risk monitoring strategy • Monitor organizational information systems and environments of operation on an ongoing basis	• Monitor and review risk factors

The NIST process includes an additional requirement for the development of a formal risk monitoring strategy that serves as a separate function within the monitoring strategy for facilitating monitoring activities through a risk monitoring program. The risk monitoring program includes features such as monitoring for compliance, effectiveness, changes, and type (automated vs. manual) and frequency of monitoring. In the ISO/IEC risk management process, an emphasis is placed on not only monitoring risks and their factors, but also monitoring the risk management process itself to ensure it is consistently applied and improvements in the process or relevance of risk criteria are integrated into the risk management approach.

SUMMARY

This chapter introduced the topic of organization-wide risk management. Risk management plays a critical role within the federal government, and the cultural adoption of information technology. The adoption of cloud services will need to be addressed by a government-wide approach in which risk management is integrated into the federal information security programs to achieve a "do once, use many times" approach.

In this chapter we were also introduced to the federal risk management practices, and how over time, the maturity of these practices evolved. Since both federal agencies and service providers may adopt different risk management processes, understanding where the differences might exist is important to cost-effectively implement risk management programs. Therefore, we concluded with a brief comparison of the harmonization between the federal risk management practices and the international risk management standards.

References

[1] Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing information security risk: organization, mission, and information system view. Maryland: National Institute of Standards and Technology; 2011.

[2] Davis R. Federal Information Processing Standard (FIPS) Publication 31, Guidelines for automatic data processing physical security and risk management. Maryland: National Bureau of Standards; 1974.

[3] Davis R. Federal Information Processing Standard (FIPS) Publication 41, Computer security guidelines for implementing the privacy act of 1974. Maryland: National Bureau of Standards; 1975.

[4] Gilbert E. NIST Special Publication (SP) 500-174, Guide for selecting automated risk analysis tools. Maryland: National Institute of Standards and Technology; 1989.

[5] Swanson M, Guttman B. NIST Special Publication (SP) 800-14, Generally accepted principles and practices for securing information technology systems. Maryland: National Institute of Standards and Technology; 1996.

[6] Brock J. Information security risk assessment, practices of leading organizations. Washington: US Government Accountability Office; 1999.

[7] Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing information security risk: organization, mission, and information system view. Maryland: National Institute of Standards and Technology; 2011.

[8] Wilshusen G. Progress made on harmonizing policies and guidance for national security and non-national security systems. Washington: US Government Accountability Office; 2010.

[9] Metheny M. [Internet]. Florida: International information systems security certification consortium [cited January 25, 2012]. <http://blog.isc2.org/isc2_blog/2010/12/cloud-adoption-risk-management.html>.

[10] Van Roekel S. Security authorization of information system in cloud computing environments. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011.

[11] Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-30 Revision 1, Guide for conducting risk assessments. Maryland: National Institute of Standards and Technology; 2011.

[12] Guttman B, Roback E. NIST SP 800-11, An Introduction to Computer Security: The NIST Handbook. Maryland: National Institute of Standards and Technology; 1996.

[13] Jansen W, Grance T. NIST Special Publication (SP) 800-144, Guidelines on Security and Privacy in Public Cloud Computing. Maryland: National Institute of Standards and Technology; 2011.

CHAPTER

Comparison of Federal and International Security Certification Standards

7

INFORMATION IN THIS CHAPTER:

- Introduction
- Overview of Certification and Accreditation
- NIST and ISO/IEC Information Security Standards

INTRODUCTION

Managing information security and compliance requirements on an audit-by-audit basis can be a challenging and difficult task, specifically where security control assessment results and evidence are gathered, analyzed, and reported simultaneously. This duplication of effort can result in significant inefficiencies and an unproductive use of resources. However, the ability to leverage reuse and satisfy multiple compliance and contractual obligations requires a comprehensive information security and compliance framework. Additionally, the framework needs to be able to harmonize compliance requirements across both the federal government and industry.

Federal agencies, contractors, and service providers are required to adhere to a variety of mandates that cut across multiple federal laws, directives, regulations, standards, and policies. In addition to the federal requirements, some service providers are required to support other compliance obligations from a number of different industry security laws, regulations, and standards. The overlap in the security requirements and compliance obligations has resulted in service providers establishing multiple, and sometimes concurrent, information security and risk management programs. Some of these programs even operate independently due to the inferred incapability, resulting in unnecessary redundancies.

The federal government has, itself, struggled with similar problems. Federal information security programs are often complex and continuously changing. In addition, the increasing reliance on external service providers for information technology (IT) services, and the duplication of certification and accreditation (C&A) processes have required the federal government to transform existing processes to one that is more unified, agile, and streamlined. One of the goals of the new process is to unify the different information security frameworks across the federal government and establish a

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00007-1

foundational set of common information security standards and guidelines. This new process would also require the involvement of a government-wide effort to continue to identify gaps and standardize federal security requirements, in addition to harmonizing with existing international security standards. Thereby creating consistency in security standards and practices to support reciprocity by enabling the federal government to leverage existing authorizations, a necessary requirement for the success of the Federal Risk and Authorization Management Program (FedRAMP).

OVERVIEW OF CERTIFICATION AND ACCREDITATION

The concept of C&A is a well-defined security methodology used both within the US government and internationally.[1] For illustrative purposes, Table 7.1 provides definitions for both *certification* and *accreditation* included in various security standards (and guidelines) used over the years from across the different federal communities (i.e., Civilian Agencies, the Department of Defense (DoD), and the Intelligence Community (IC)).[2] In reviewing the definitions, one can identify a common definitional purpose for the C&A process, even though the policies, procedures, and practices may be uniquely developed to desribe how the different C&A processes are implemented for use within each of the federal communities. Therefore, a common definition of the C&A process can be summarized as follows:

> *A process for evaluating (or assessing) the technical and non-technical security safeguards (or controls) implemented to protect the information technology systems or applications against threats and vulnerabilities to achieve an acceptable level of risk.*

In the next section, we will examine each of the federal C&A processes to gain a better understanding of how the federal government's security practices have evolved over time. In addition, the examination will serve to provide an insight into the significant challenges that exist for establishing and maintaining a standardized process that will be necessary to achieve reciprocity required for the cost-effective use of FedRAMP provisionally authorized cloud services.[3]

[1] As an example is ISO/IEC 27001:2005, originally developed by the British Standards Institute (or the BSI Group's British Standards) BS7799-2:1998 in February 1998, an internationally recognized certification process for an organization's Information Security Management System (ISMS).

[2] From Wilshusen, G. Progress Made on Harmonizing Policies and Guidance or National Security and Non-National Security Systems. Washington: US Government Accountability Office; 2010. *"The intelligence community is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States."*

[3] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. "Reciprocity is the mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. Reciprocity is best achieved by promoting the concept of transparency (i.e., making sufficient evidence regarding the security state of an information system)."

Table 7.1 Definitions of Certification[a] and Accreditation[c]

Date	Certification	Accreditation
1983[b]	A technical evaluation that establishes the extent to which a computer system or network design implementation meets a prespecified set of security requirements [1].	The authorization and approval granted to a system or network to process sensitive data in an operational environment [1].
1994	"A comprehensive analysis of the technical and nontechnical security features and other safeguards of a system to establish the extent to which a particular system meets a set of specified security requirements" [2].	"A formal declaration by a designated approving authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards"[2].
2000	"Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements"[3].	"Formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk" [3].
2000	"Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements" [4].	"Formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk" [4].
2004	"A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system" [5].	"The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls" [5].
2007	"A comprehensive evaluation and validation of a DoD IS to establish the degree to which it complies with assigned IA controls based on standardized procedures" [6].	"A formal statement by a designated accrediting authority (DAA) regarding acceptance of the risk associated with operating a DoD information system (IS) and expressed as an authorization to operate (ATO), interim ATO (IATO), interim authorization to test (IATT), or denial of ATO (DATO)" [6].

Table 7.1 Definitions of Certification[a] and Accreditation[c] (*Continued*)

Date	Certification	Accreditation
2008	"A comprehensive assessment of the management, operational, and technical security controls in an information technology system, or for a particular item of information technology, made in support of accreditation" [7].	"Official management decisions that explicitly accept a defined level of risk associated with the operation of an information technology system at a particular level of security in a specific environment on behalf of an IC element" [7].
2010	A determination of the "extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system" [8].	"The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls" [8].
2010	"Comprehensive evaluation of the technical and non-technical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements" [9].	"Formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards" [9].

[a] *Synonymous with security control assessment in some NIST, DoD, and CNSS references.*

[b] *FIPS 39, Glossary for computer systems security.*[c] *Synonymous with security authorization in some NIST, DoD, and CNSS references.*

Evolution of the Federal C&A Processes

Federal agencies are continuing to improve the ways to which they interconnect information systems. In recent years, federal agencies have begun to use more agile development methodologies to maintain pace with quickly evolving technology architectures. Using agile methodologies also enables the federal government to be more adaptable and better equipped to support changes in their mission and business requirements. Similar to the technology changes discussed in Chapter 1, as early as the 1970s, C&A processes used by the federal government have also evolved. The evolution of C&A processes and practices has been established through the development of a number of different standards (and guidelines). However, these processes and practices have also been applied differently, both between federal communities and federal agencies within the same community.[4]

In the remainder of this section, we will focus our discussion through a brief overview of the different C&A processes that have been used across the federal government with the intent of gaining an understanding into how they evolved and were changed. However, this section is not meant to be a comprehensive tutorial of the federal C&A processes, but instead it will serve to provide a summary of how information security and risk management practices have evolved and were implemented independently across the different federal communities.

Civilian Agencies

In 1983, the National Bureau of Standards (NBS), now known as National Institute of Standards and Technology (NIST), published the Federal Information Processing Standard (FIPS) PUB 102, "*Guideline for Computer Certification and Accreditation.*" This publication provided federal agencies with a guide for establishing and carrying out a program and a technical process for computer security C&A.[5] [1] The key purpose of the publication was to achieve two main objectives:

- Establishing a program for certification and accreditation (e.g., policies and procedures, and roles and responsibilities); and
- Performing a certification and accreditation (e.g., planning, data collection, evaluation, and reporting findings).

[4] From Wilshusen, G. Progress Made on Harmonizing Policies and Guidance or National Security and Non-National Security Systems. Washington: US Government Accountability Office; 2010. *"Prior to efforts to harmonize information security guidance, federal organizations had developed separate, and sometimes disparate, guidance for information security. For example, the National Security Agency used the National Information Systems Certification and Accreditation Process, the intelligence community used DCID 6/3, and DOD used the Department of Defense Information Technology Security Certification and Accreditation Process, which later became the DIACAP."*

[5] From Burrows, J. Federal Information Processing Standard (FIPS) PUB 102, Guidelines for Computer Security Certification and Accreditation. Maryland: National Institute of Standards and Technology; 1983. *"The quality exhibited by a computer system that embodies its protection against internal failures, human errors, attacks, and natural catastrophes that might cause improper disclosure, modification, destruction, or denial of service."*

The FIPS PUB 102 C&A process became the standard of practice for use by civilian federal agencies until 2004, when NIST published the first version of the Special Publication (SP) 800-37, "*Guide for the Security Certification and Accreditation of Federal Information Systems.*"

During the period between the publication of FIPS PUB 102 and NIST SP 800-37, the Federal Information Security Management Act (FISMA)[6] became law (2002). As a result of the gap in guidance, OMB released a memo through the Federal Chief Information Officers (CIO) Council to provide interim guidance for federal agencies until NIST published SP 800-37. This memo gave federal agencies the freedom to use another comparable security certification methodology provided it addressed the requirements covered in NIST SP 800-26 [10].[7]

When the first version of NIST SP 800-37 was published, it became the standard guidance used by civilian federal agencies for non-National Security Systems (NSSs) until the C&A process was revised in February 2010 through an updated version of NIST SP 800-37 (Revision 1). Although this new publication, led by NIST, was created through the Joint Task Force Transformation Initiative (JTFTI) Interagency Working Group. As will be revisited in a later section, the goal of the JTFTI was the development of a common set of core standards and guidelines that would be part of a government-wide C&A transformation effort. This new effort aimed at modernizing the traditional C&A process through the elimination of separate processes and the implementation of a risk-based security authorization approach. This new approach focused on creating a common information security framework that could be used across the federal government.[8] In addition, the focus was to make the process more dynamic by enabling near, real-time risk management and continuous monitoring through a single Risk Management Framework (RMF).[9]

[6] FISMA was discussed in detail in Chapter 5, Applying the NIST Risk Management Framework.

[7] NIST Special Publication (SP) 800-26, Security Self-Assessment Guide for Information Technology Systems, published in 2001, built upon the Federal IT Security Assessment Framework published by the Federal CIO Council in 2000 as a tool for use by federal agencies when evaluating their IT security programs. NIST Special Publication (SP) 800-26 was superseded by Federal Information Processing Standard (FIPS) 200/NIST Special Publication (SP) 800-53 (specification of security controls) and NIST Special Publication (SP) 800-53A (assessment of security control effectiveness).

[8] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"NIST in partnership with the Department of Defense (DoD), the Office of the Director of National Intelligence (ODNI), and the Committee on National Security Systems (CNSS), has developed a common information security framework for the federal government and its contractors."*

[9] The RMF was discussed in detail in Chapter 5, Applying the NIST Risk Management Framework.

Department of Defense (DoD)

In 1994, the National Computer Security Center (NCSC),[10] originally known as the DoD Computer Security Center (CSC), a part of the National Security Agency (NSA), published the "*Introduction to Certification and Accreditation*" (or the "Blue Book"). This book was one of many standards and guidelines included within the *"Rainbow Series"*[11] and provided a high-level introduction for both the DoD and non-DoD communities on the basic concepts and policies associated with C&A, including roles and responsibilities and the risk management process. Following the publication of the "Blue Book," the "*Certification and Accreditation Process Handbook for Certifiers*" was published to provide more focused guidance on creating a "structured process by which to perform a C&A of a system" [10].

However, it was not until 1997 through the Defense-wide Information Security Program (DISSP)[12] that a DoD-wide C&A process was created. This new process, which became known as the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), was expected to be the standard C&A process for use across the DoD. DITSCAP not only established a standard process to certify and accredit information systems, but was also to be used to maintain the security posture of the Defense Information Infrastructure (DII) through an infrastructure approach to C&A [11].

After FISMA became law, the DoD C&A process changed again. In 2006, through an interim instruction, DITSCAP began the transition to a new dynamic process known as the Defense Information Assurance Certification and Accreditation Process (DIACAP). DIACAP, through a final official issuance in 2007, was designed as the DoD-wide C&A process to be used to support the transition of DoD information systems to Global Information Grid (GIG)[13] standards and a net-centric environment. In addition, this new process had the objective of enabling improved information sharing across the DoD through a standard C&A approach that focused on providing specific DoD-wide guidance on managing and disseminating enterprise standards and guidelines for IA design, implementation, configuration, validation, operation sustainment, and reporting [12].

[10] From Gallagher, P. NCSC-TG-031 Version 1, Certification and Accreditation Process Handbook for Certifiers. Maryland: National Computer Security Center; 1996. *The Introduction to Certification and Accreditation and the Certification and Accreditation Process Handbook for Certifiers were not developed specifically for the DoD, but instead provided guidance that could be used by DoD and Non-DoD agencies and organizations.*

[11] *Rainboww Series*. Available from: http://csrc.nist.gov/publications/secpubs/rainbow/.

[12] The Defense-wide Information Security Program (DISSP), currently known as the Defense-wide Information Assurance Program (DIAP), is a part of the Defense Information Systems Agency (DISA), Center for Information Systems Security (CISS).

[13] From England, G. DoDI 8000.01, Management of the Department of Defense Information Enterprise. Washington, DC: Department of Defense; 2009. *"The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."*

Intelligence Community (IC)

The Director of Central Intelligence Directives (DCID), issued by the Director of Central Intelligence (DCI), were formerly used to provide intelligence community-wide policies and guidance, including governing information systems that stored, processed, or transmitted intelligence information. In 1983, DCID 1/16 was published (and later updated in 1988) by the DCI to establish a security policy for the processing, storage, and transmission of US foreign intelligence and counterintelligence in automated information systems (AIS) and networks. Additionally, the criteria in the DoD Trusted Computer System Evaluation Criteria (TCSEC), published by the NCSC in 1985, was identified by DCID 1/16 as the protective measures (administrative, environmental, and technical security requirements) that were required to be met by the AIS to protect sensitive information. However, DCID 1/16 later became superseded by DCID 6/3[14] in 1999, with an implementation manual being published in 2000[15] (and an update in 2002). DCID 6/3 became the first C&A process documented for use by the IC.

DCI policy was used within the IC until the establishment of the Office of the Director of National Intelligence (ODNI) in 2005. In 2008, the ODNI published the Intelligence Community Directive (ICD) 503, which was to supersede DCID 6/3.[16] The ICD 503 was established to implement the strategic goals[17] agreed upon by the IC CIO, the DoD CIO, OMB, and NIST. ICD 503 and other transition guidance in the form of directives and standards directed the use of CNSS policy and guidance, which in turn pointed to the harmonized NIST guidance [13].

Committee on National Security Systems (CNSS)

The CNSS[18] published the National Information Assurance Certification and Accreditation Process (NIACAP) in 2000. The NIACAP process, with similarities to the DITSCAP, was used by Civilian Agencies for NSS[19] for both national telecommunication and

[14] DCID 6/3 was developed to be a harmonization with DITSCAP.

[15] DCID 6/3, Manual, Protecting Sensitive Compartmented Information within Information Systems, April 2002.

[16] Although ICD 503 directed the use of polices and guidance created by the CNSS and NIST, respectively, DCID 6/3 is still widely used within the IC.

[17] From Public Affairs Office. ODNI News Release No. 10-07, DNI & DoD Chief Information Officers Announce Certification and Accreditation Transformation Goals. Washington, DC: Office of the Director of National Intelligence; 2007. *One of the goals was the institute of a common C&A that "will ensure system certifications and accreditations accomplished by one agency are valid for all agencies."*

[18] From Office of the Director of National Intelligence [Internet]. Maryland: Committee for National Security Systems, [cited 2012 Febraury 15]. Available from: http://www.cnss.gov/history.html. *"The Committee on National Security Systems (CNSS), formerly named the National Security Telecommunications and Information Systems Security Committee (NSTISSC), provides a forum for the discussion of policy issues, and has the responsibility for setting national-level Information Assurance policies, directives, instructions, operational procedures, guidance, and advisories for US Government (USG) departments and agencies for the security of National Security Systems (NSS)."*

[19] NSSs were briefly discussed in Chapter 5. However, NIST Special Publication (SP) 800-59, *"Guide for Identifying an Information System as a National Security System,"* provides additional guidance for the identification of NSSs.

information systems. In 2005, the CNSS issued the "*National Policy on Certification and Accreditation of National Security Systems*" to give civilian federal agencies the flexibility to use NIACAP or an alternative C&A process. Since the CNSS is also a part of the JTFTI Interagency Working Group, it is "working with representatives from the Civil, Defense, and Intelligence Community to produce a unified information security framework" [14]. As a first step, CNSS Policy No. 22[20] was issued, establishing a requirement for the use of an organization-wide IA risk management program for all NSSs that is consistent with the NIST standards and guidelines.

NOTE

Outside of the application of C&A processes on traditional information systems, there also exist C&A processes for interfaces used to control access or transfer information between differing security domains. The Secret and Below Interoperability (SABI) and the Top Secret/Sensitive Compartmented Information (SCI) and Below Interoperability (TSABI) processes have been developed by the DoD and IC for addressing risk associated with operating cross-domain solutions (CDS)[21] that control the connection between networks of different classification levels.

- SABI C&A process follows the DIACAP C&A principles.
- TSABI C&A process follows the DCID 6/3 C&A principles.

In an effort to unify the two processes, the Unified Cross Domain Management Office (UCDMO), was created "to more effectively share information between security domains—that is, to move information between networks at different clearance (classification) levels throughout the federal government" [15]. The UCDMO, in an effort to unify the security requirements, published the CDS Overlay in December 2011, which provides a single comprehensive set of security control guidance for CDS. The CDS Overlay is based on the NIST SP 800-53 Revision 3 and the CNSS-1253.

In addition, the NIST SP 800-53 Revision 4 (IPD) described CDSs as potential situations where additional conditions and controls might be required:

"Security control baselines do not assume that information systems have to operate across multiple security policy domains. The baselines assume a flat view of information flows (i.e. the same security policies in different domains when information moves across authorization boundaries). To address cross-domain services and transactions, some subset of the AC-4 security control enhancements can be considered to ensure adequate protection of information when transferred between information systems with different security policies" [16].

[20] From Takai, T. CNSSP No. 22, Policy on Information Assurance Management for National Security Systems. Maryland: Committee on National Security Systems; 2012. *"Upon this revision of CNSSP No. 22, CNSS Policy No. 6, "National Policy on Certification and Accreditation of National Security Systems," dated October 2005, and National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000, "National Information Assurance Certification and Accreditation Process (NIACAP)" were canceled.*

[21] From Unified Cross Domain Management Office (UCDMO) [Internet]. Maryland: Unified Cross Domain Management Office (UCDMO); [cited 2012 Feb 15]. Available from: http://www.ucdmo.gov/faqs.html. *"Cross Domain Solutions (CDS) are controlled interfaces that provide the capability to access or transfer information across different security domains. (Unclass to Secret, Secret to Top Secret, etc.)."*

Towards a Unified Approach to C&A

As previously mentioned, the JTFTI, led by NIST, with participating members from the Civilian, Defense, and Intelligence Communities, is a joint partnership focused on transforming the federal government's C&A processes. One of the primary goals is to establish a "unified information security framework that harmonizes security standards and guidelines for NSSs and non-NSSs" [13]. This harmonization effort not only eliminates the duplication among the various federal C&A processes, but is also aims at reducing the cost associated with managing and operating multiple overlapping C&A processes.

In addition, the unified process will enable the government to more effectively share information when responding to the growing number of advanced cyber threats.

These cyber threats have led to challenges within the federal government's ability to seamlessly share information and authorizations through reciprocity, effectively limiting the reuse of evidence when verifying the implementation of security controls between interconnected systems. As depicted in Figure 7.1, the unification of C&A processes establishes a bridge across the various federal communities by harmonizing policies and guidance. This harmonization process focuses on using the NIST standards and guidelines currently applied to non-NSSs, leaving the DoD and IC to

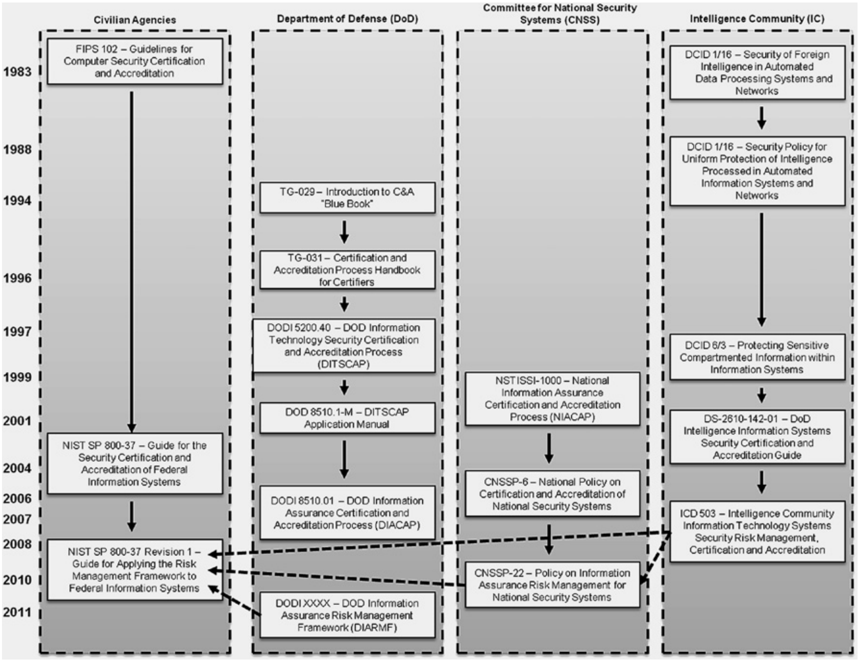

Civilian Agencies
Department of Defense (DoD)
Committee for National Security Systems (CNSS)
Intelligence Community (IC)
1983
1988
1994
1996
1997
1999
2001
2004
2006
2007
2008
2010
2011
FIPS 102 – Guidelines for Computer Security Certification and Accreditation
NIST SP 800-37 – Guide for the Security Certification and Accreditation of Federal Information Systems
NIST SP 800-37 Revision 1 – Guide for Applying the Risk Management Framework to Federal Information Systems
TG-029 – Introduction to C&A "Blue Book"
TG-031 – Certification and Accreditation Process Handbook for Certifiers
DODI 5200.40 – DOD Information Technology Security Certification and Accreditation Process (DITSCAP)
DOD 8510.1-M – DITSCAP Application Manual
DODI 8510.01 – DOD Information Assurance Certification and Accreditation Process (DIACAP)
DODI XXXX – DOD Information Assurance Risk Management Framework (DIARMF)
NSTISSI-1000 – National Information Assurance Certification and Accreditation Process (NIACAP)
CNSSP-6 – National Policy on Certification and Accreditation of National Security Systems
CNSSP-22 – Policy on Information Assurance Risk Management for National Security Systems
DCID 1/16 – Security of Foreign Intelligence in Automated Data Processing Systems and Networks
DCID 1/16 – Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks
DCID 6/3 – Protecting Sensitive Compartmented Information within Information Systems
DS-2610-142-01 – DoD Intelligence Information Systems Security Certification and Accreditation Guide
ICD 503 – Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation

FIGURE 7.1 Civilian Agency, DoD, and IC C&A Processes

NOTE

The DoD Cloud Computing Strategy, published by the DoD CIO,[22] directed leveraging efforts such as FedRAMP, which prescribes the use of the NIST standards and guidelines as a standardized and streamlined C&A process for commercial and federal cloud providers [18].

shift their focus to addressing the unique security requirements through community-specific[23] policies and guidance.

NOTE

There are several key differences between the information and system categorization steps and the control selection processes described between the CNSS policies and the NIST standards and guidelines. These differences [13] include:

- *System Categorization*—different methodologies[24] are used to categorize the impact associated with information that is stored, processed, or transmitted.
- *Security Control Selection*—selection of control baselines or control profiles will be conducted differently within each of these communities.
- *Program Management Controls*—program management controls required for non-national information security programs will be optional for national security system information security programs.

NIST AND ISO/IEC INFORMATION SECURITY STANDARDS

In the last section we discussed an effort to transition towards a common government-wide foundation for information security using the NIST standards (and guidelines). In this section, the discussion will focus on the harmonization between the NIST standards (and guidelines) and the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) information

[22] The DoD CIO is also a permanent member of the FedRAMP Joint Authorization Board (JAB), along with the CIO of the US Department of Homeland Security (DHS) and the US General Services Administration (GSA). Available from: http://www.gsa.gov/graphics/staffoffices/FedRAMP_JAB_Charter_SIGNED.pdf.

[23] From Wilshusen, G. Progress Made on Harmonizing Policies and Guidance or National Security and Non-National Security Systems. Washington: US Government Accountability Office; 2010. *"FISMA provides a further exception to compliance with NIST standards. It permits an agency to use more stringent information security standards if it certifies that its standards are at least as stringent as the NIST standards and are otherwise consistent with policies and guidelines issued under FISMA."*

[24] From Shaeffer, R. CNSS Instruction No. 1253, Security Categorization and Control Selection for National Security Systems. Maryland: Committee on National Security Systems; 2009. In the National Security Community, the potential impact levels determined for confidentiality, integrity, and availability are retained, meaning there are 27 possible three-value combinations for NSI or NSS, as opposed to the three possible single-value categorizations obtained using the guidelines in FIPS 200. Retaining the discrete impact levels for each of the three security objectives is done to provide a better granularity in allocating security controls to baselines, and should thereby reduce the need for subsequent tailoring of controls.

security standards, [25] which are widely adopted for use within the private sector[26] for addressing information security and risk management. The NIST security standards (and guidelines)[27] provide a framework for a mandatory certification process directed by FISMA[28] to authorize information systems for use by both federal agencies and contractors. Whereas, the ISO/IEC standards provide a voluntary certification process for use by non-government organizations to confirm their management system incorporating generally-accepted information security best practices. For comparison, Table 7.2 provides a list of major references that have been published by NIST and the ISO/IEC for implementing the different components of a comprehensive information security and risk management program.

In previous chapters we examined both the NIST RMF[29] and the NIST Risk Management[30] process. In this section, the discussion will shift to provide a basic understanding of the relationship between the different information security and risk management standards, focusing on highlighting their compatibility, but limiting the discussion of recommending any specific methods and methodologies for aligning or integrating the different processes. To support the discussion, Figure 7.2 provides a point of reference for use by service providers that have already invested in becoming certified or are currently operating under the ISO/IEC standards. By defining the relationship between the different information security and risk management standards, service providers will be better positioned to align their information security programs, and enabling them to reuse their exiting investment.

Boundary and Scope Definition

The NIST RMF and the ISO/IEC “Plan-Do-Check-Act” (PDCA) focuses on applying a structured, risk-based approach for the integration of information security. Both NIST (*800-37 Revision 1—RMF Step 1*) and the ISO/IEC (*27001—Clause 4.2.1.a*)

[25] From Powner, D. Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. Washington: US Government Accountability Office; 2010. *“The IEC and the International Organization for Standardization (ISO), through a joint technical committee (JTC), have developed information security standards for all types of organizations, including commercial enterprises, government agencies, and not-for-profit organizations.”*

[26] The Information Security Management System (ISMS) is a systematic approach that includes the policies, peoples, processes practices, and technologies for managing information security risks affecting the confidentiality, integrity, and availability.

[27] Federal Information Security Standards (FIPS) and NIST Special Publication (SP) 800 series.

[28] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2012. *“Although the NIST security standards (and guidelines) were developed in response to FISMA they are consistent with ISO/IEC 27001, but provide additional implementation detail for use by the federal government and its contractors.”*

[29] See Chapter 5, Applying the Risk Management Framework.

[30] See Chapter 6, Risk Management.

Table 7.2 Mapping of Information Security and Risk Management Programs to NIST and ISO/IEC Standards (and Guidelines)

Component	NIST	ISO/IEC
Risk Management (*including Risk Assessment Methodology*)	• NIST SP 800-39—Managing Information Security Risk: Organization, Mission, and Information System View • NIST SP 800-30 Revision 1—Guide for Conducting Risk Assessments	• ISO/IEC 30000—Risk management—Principles and guidelines • ISO/IEC 30010—Risk assessment techniques • ISO/IEC 27005—Information technology—Security techniques—Information security risk management
Information Security Framework	• NIST SP 800-37—Guide for Applying the Risk Management Framework to Federal Information Systems	• ISO/IEC 27001—Information technology—Security techniques—Information security management systems—Requirements
Information Security Controls	• NIST SP 800-53—Recommended Security Controls for Federal Information Systems and Organizations	• ISO/IEC 27002—Information technology—Security techniques—Code of practices for information security management
Information Security Assessment/Auditing	• NIST SP 800-53A—Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans	• ISO/IEC 27007—Information technology—Security techniques—Guidelines for information security management systems auditing • ISO/IEC 27008—Information technology—Information technology—Security techniques—Guidelines for auditors on information security management systems controls

require the identification of a boundary[31] around the information system.[32] However, within the ISO/IEC process, the scope (or boundary) typically includes the organization

[31] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *Authorization boundary is "all components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected."*

[32] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"A discrete set of information resources (e.g. personnel and information technology) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."*

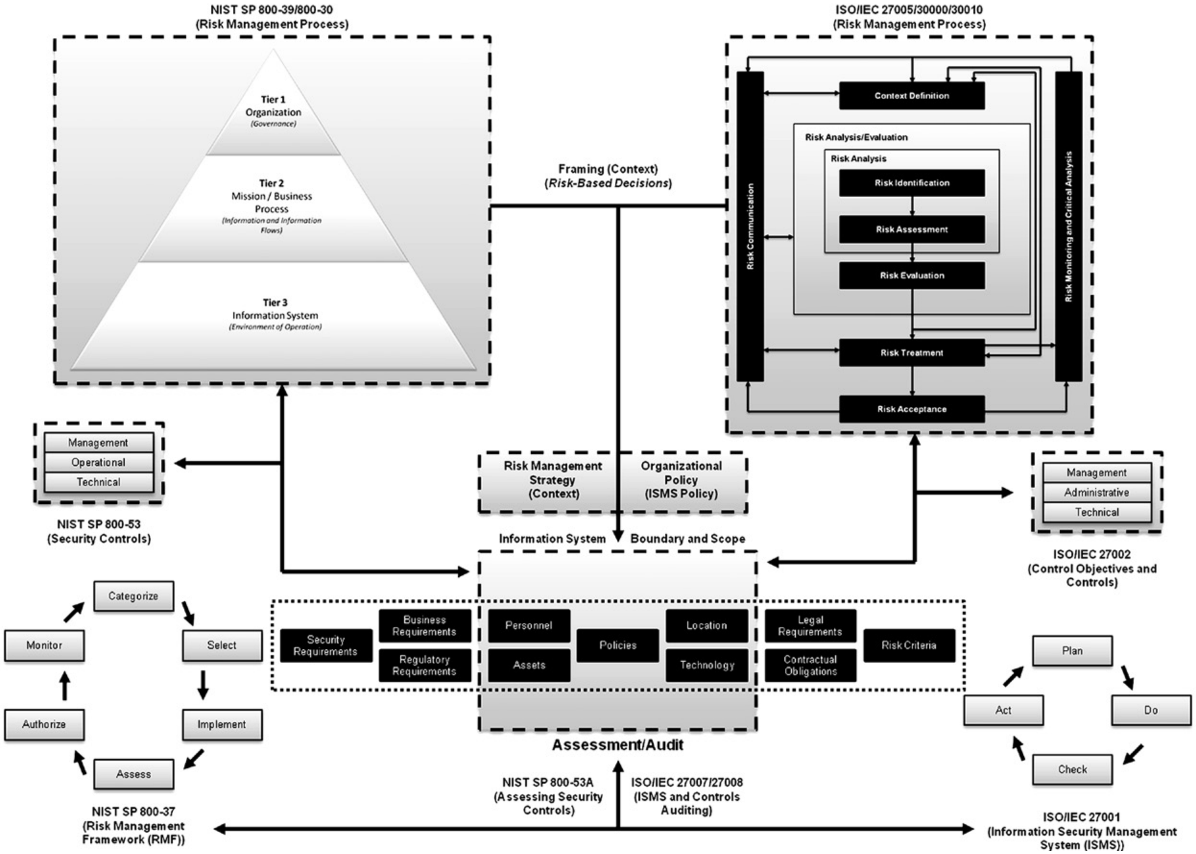


FIGURE 7.2 Relationship between NIST and ISO/IEC Information Security Standards

NOTE

The NIST FISMA Implementation Project includes several initiatives under the second phase (Phase II: Implementation and Assessment Aids) of the project. The ISO Harmonization Initiative focuses on identifying common relationships and mappings of FISMA standards, guidelines, and requirements with: (i) ISO/IEC 27000 series information security management standards; and (ii) ISO/IEC 9000 and 17000 series quality management, and laboratory testing, inspection and accreditation standards. This harmonization is important for minimizing duplication of effort for organizations that must demonstrate compliance to both FISMA and ISO requirements [19].

and the information system which maintains and has control over the information system. To effectively characterize the boundary and scope of protection,[33] processes require the organization to define the associated policies,[34] assets, technologies, locations, and personnel.

Security Policy

After the boundary and scope have been defined, the organization creates an information security policy (*addressed through the NIST SP 800-53 XX-1 controls and the ISMS policy*[35]*in ISO/IEC 27001*), which establishes the management's direction and principles for governing the information system. In addition, the security policy[36] should, at a minimum, include a purpose and scope *(SP 800-53 XX-1 controls)*, identify the roles and responsibilities (*SP 800-53 XX-1 controls and 27001—A.6.1.3)*, address a statement of compliance that is supported through a management commitment *(SP 800-53 XX-1 controls and 27001—A.6.1.1)*, and coordinate among organizational entities *(SP 800-53 XX-1 controls and 27001—A.6.1.2)*.

[33] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"Well-defined boundaries establish the scope of protection for organizational information systems (i.e. what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes."*

[34] From Burrow, J. McNulty, F., Katzke, S. Gilbert, I., and Steinauer, D. NIST Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook. Maryland: National Institute of Standards and Technology; 1995. *A "senior management's directives to create a computer security program, establish its goals, and assign responsibilities."*

[35] ISMS policy can include all of the security policies.

[36] From Bowen, P., Hash, J., and Wilson, M. NIST Special Publication (SP) 800-100, Information Security Handbook: A Guide for Managers. Maryland: National Institute of Standards and Technology; 2006. *"An aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information."*

NOTE

In NIST SP 800-53, "*Recommended Security Controls for Federal Information Systems and Organizations,*" the first control in each control family[37] (e.g., Access Controls, Identification and Authentication, Incident Response, etc.) requires identifying the policies and procedures that are implemented by the remaining security controls (and control enhancements) included in the family of controls.

The policies may be inherited completely (common control[38]) from the organizational policies or may be derived partially (hybrid control[39]) from an organizational policy that is further defined in an information system-specific policy.

Risk Management Strategy (Context)

Both NIST and ISO/IEC require an organizational policy (or ISMS policy) that aligns with the risk management strategy[40] (or context). The risk management strategy is developed as an output of the risk framing (or context definition). The framing[41] (context) definition is established as a part of the risk management process[42] discussed in Chapter 6.

Risk Management Process

Before the allocation[43] of the security controls, the organization needs to understand the risks by conducting a risk assessment. Both NIST (*800-37 Revision 1—RMF*

[37] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology, 2010. *"A control family is associated with a given class based on the dominant characteristics of the controls in that family."*

[38] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"A security control that is inherited by one or more organizational information systems."*

[39] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"A security control that is implemented in an information system in part as a common control and in part as a system-specific control."*

[40] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"How the organization intends to assess risk, respond to risk, and monitor risks."*

[41] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Describes the environment in which risk-based decisions are made."*

[42] See Chapter 6 for a comparison of the NIST and ISO/IEC Risk Management processes.

[43] Allocation of security controls can occur by assigning responsibility for security controls at each of the three tiers (governance, mission/business process, or information system levels) in the risk management hierarchy.

Table 7.3 Comparison of Options for Risk Response or Treatment

NIST	ISO/IEC
• Risk Acceptance • Risk Avoidance • Risk Sharing • Risk Transfer	• Risk Reduction • Risk Retention • Risk Avoidance • Risk Transfer

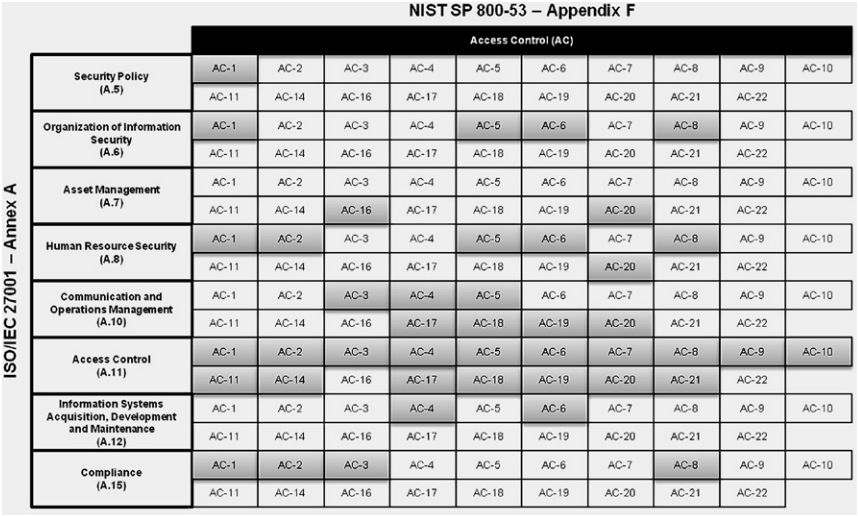
Step 2) and the ISO/IEC (*27001—Clause 4.2.1.d-g*) address the selection of security controls before and after the risk assessment. In addition, NIST and the ISO/IEC have a separate function within the risk management process (discussed in Chapter 6) where the risks are evaluated based on criteria established during the framing (or context definition) step. This criterion assists in determining which of the risk response (or risk treatment) options in Table 7.3 would be appropriate as a treatment for the risk.

One notable difference between the NIST and ISO/IEC processes is the explicit requirements for the acceptance of risk defined in the risk treatment plan and the residual risk acceptance. For example, NIST does specify the acceptance of risk; it is performed as a result of the approval of the system security plan (*800-37 Revision 1—RMF Step 3*) and authorization to operate (*800-37 Revision 1—RMF Step 5*). However, both the NIST and ISO/IEC risk management processes include the ongoing monitoring where risk management becomes a continual process.[44]

Security Objectives and Controls

The selection (and implementation) of control objectives and controls is a similar activity under both the NIST and ISO/IEC processes. The selection process focuses on identifying those control objectives and controls that meet the requirements of the organizational assessment of risk identified during the execution of the risk assessment, in addition to requirements derived from other sources such as business requirements, regulatory requirements, legal requirements, and contractual obligations. One significant difference that exists is in the scope and organization of the security controls included in NIST security control families (*800-53—Appendix F*) and the ISO/IEC security control clauses (*27001—Annex A*). In Figure 7.3, a

[44] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes."*



NIST SP 800-53 – Appendix F

ISO/IEC 27001 – Annex A	Access Control (AC)									
Security Policy (A.5)	**AC-1**	AC-2	AC-3	AC-4	AC-5	AC-6	AC-7	AC-8	AC-9	AC-10
	AC-11	AC-14	AC-16	AC-17	AC-18	AC-19	AC-20	AC-21	AC-22	
Organization of Information Security (A.6)	**AC-1**	AC-2	AC-3	AC-4	**AC-5**	**AC-6**	AC-7	**AC-8**	AC-9	AC-10
	AC-11	AC-14	AC-16	AC-17	AC-18	AC-19	AC-20	AC-21	AC-22	
Asset Management (A.7)	AC-1	AC-2	AC-3	AC-4	AC-5	AC-6	AC-7	AC-8	AC-9	AC-10
	AC-11	AC-14	**AC-16**	AC-17	AC-18	AC-19	**AC-20**	AC-21	AC-22	
Human Resource Security (A.8)	**AC-1**	**AC-2**	AC-3	AC-4	**AC-5**	**AC-6**	AC-7	**AC-8**	AC-9	AC-10
	AC-11	AC-14	AC-16	AC-17	AC-18	AC-19	**AC-20**	AC-21	AC-22	
Communication and Operations Management (A.10)	AC-1	AC-2	**AC-3**	**AC-4**	**AC-5**	AC-6	AC-7	AC-8	AC-9	AC-10
	AC-11	AC-14	AC-16	**AC-17**	**AC-18**	**AC-19**	**AC-20**	AC-21	AC-22	
Access Control (A.11)	**AC-1**	**AC-2**	**AC-3**	**AC-4**	**AC-5**	**AC-6**	**AC-7**	**AC-8**	**AC-9**	**AC-10**
	AC-11	**AC-14**	AC-16	**AC-17**	**AC-18**	**AC-19**	**AC-20**	**AC-21**	AC-22	
Information Systems Acquisition, Development and Maintenance (A.12)	AC-1	AC-2	AC-3	**AC-4**	AC-5	**AC-6**	AC-7	AC-8	AC-9	AC-10
	AC-11	AC-14	AC-16	AC-17	AC-18	AC-19	AC-20	AC-21	AC-22	
Compliance (A.15)	**AC-1**	**AC-2**	**AC-3**	AC-4	AC-5	AC-6	AC-7	**AC-8**	AC-9	AC-10
	AC-11	AC-14	AC-16	AC-17	AC-18	AC-19	AC-20	AC-21	AC-22	

FIGURE 7.3 Mapping of NIST (AC Security Controls) and ISO/IEC Control Objectives and Controls

mapping is provided that illustrates, in a high-level comparison, the security-related areas covered in the NIST standards (and guidelines) and the security topics included in ISO/IEC standards.

NOTE

The NIST SP 800-53 AC-1 security control requirement states:

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy.

The mapping illustrates the distinct differences between the organization of control objectives and controls included in ISO/IEC 27001 and NIST SP 800-53. For example, the AC control family is defined as follows: “Organizations must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise” [17].

When expanding the mapping of the AC family of controls, the AC controls are distributed among the various security topics (*27001—Annex A*). Some of the AC controls (e.g., AC-1) are covered in multiple ISO/IEC security objectives.

The AC-1 control requirement, as depicted in Table 7.4, provides a mapping with the ISO/IEC standards covered in the multiple control objectives and controls in Figure 7.3.

Once the control objectives and controls have been selected, they need to be documented through a System Security Plan (*800-37 Revision 1—RMF Step 2*) and the Statement of Applicability (*27001—Clause 4.2.1.j*). Although the specification of the formats may differ, the specific scope as outlined in Table 7.5 provides a general comparison of the requirements.

Table 7.4 Example Comparison of NIST (AC-1) and ISO/IEC (27001) Requirements

NIST	ISO/IEC
Control: The organization develops, disseminates, and reviews/updates *[Assignment: organization-defined frequency]*:	
a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	• A.5.1.1 Information security policy • A.11.1.1 Access control policy • A.5.1.2 Review of the information security policy • A.6.1.1 Management commitment to information security • A.6.1.3 Allocation of information security responsibilities • A.8.1.1 Roles and responsibilities • A.15.2.1 Compliance with security policies and standard
b. Formal, *documented procedures* to facilitate the implementation of the access control policy and associated access controls	• A.10.1.1 Documented operating procedures

Table 7.4 Example Comparison of NIST (AC-1) and ISO/IEC (27001) Requirements (*continued*)

NIST	ISO/IEC
Supplemental Guidance: This *control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance*. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy.	• A.10.8.1 Information exchange policies and procedures[a] • A.11.2.1 User registration[b] • A.11.2.2 Privilege management[c] • A.11.4.1 Policy on use of network services[d] • A.11.7.1 Mobile computing and communications[e] • A.11.7.2 Teleworking[f] • A.15.1.1 Identification of applicable legislation

[a] *AC-2 ("Account Management"), IA-5 ("Authenticator Management"), PE-2 ("Physical Access Authorizations").*

[b] *AC-3 ("Access Enforcement"), AC-4 ("Information Flow Enforcement"), AC-17 ("Remote Access"), AC-18 ("Wireless Access"), AC-20 ("Use of External Information Systems"), CA-3 ("Information System Connections"), PL-4 ("Rules of Behavior"), PS-6 ("Access Agreements"), SC-7 ("Boundary Protection"), SI-9 ("Information Input Restrictions").*

[c] *AC-2 ("Account Management"), AC-6 ("Least Privilege"), PE-2 ("Physical Access Authorizations"), SI-9 ("Information Input Restrictions").*

[d] *AC-5 ("Separation of Duties"), AC-6 ("Least Privilege"), AC-17 ("Remote Access"), AC-18 ("Wireless Access"), AC-20 ("Use of External Information Systems").*

[e] *AC-17 ("Remote Access"), AC-18 ("Wireless Access"), AC-19 ("Access Control for Mobile Devices"), PL-4 ("Rules of Behavior"), and PS-6 ("Access Agreements").*

[f] *AC-4 ("Information Flow Enforcement"), AC-17 ("Remote Access"), AC-18 ("Wireless Access"), PE-17 ("Alternate Work Site"), PL-4 ("Rules of Behavior"), and PS-6 ("Access Agreements").*

Table 7.5 Comparison of SSP and SOA Requirements

NIST	ISO/IEC
• Security control title • Security controls implemented or planned to be implemented • Scoping guidance applied and what type of consideration • Indication of common control and the responsible party for its implementation	• Selected control objective and controls • Reason for selection • Identification of those currently implemented • Exclusions and justification of exclusion

SUMMARY

This chapter introduced the federal C&A processes. These processes, which have evolved over time, have been used by federal agencies to certify and accredit their information systems. More recently these processes have followed a multi-year process of convergences into a single unified process, led by NIST and supplemented by community-driven requirements to accommodate specific security requirements and information sensitivity.

In addition to the federal certification standards, the ISO/IEC has developed a comparable set of standards which have been used by the private sector and internationally, and includes a similar process for certifying the organizations' information systems. The ISO/IEC process requires the implementation, operation, monitoring, review, and maintenance of an ISMS that is adequately protected based on information security requirements determined by a risk assessment and other applicable requirements (e.g., business, regulatory, contractual, and legal).

As the security and compliance requirements consistently grow and change, organizations will have to adjust their approaches, tools, and techniques to ensure not only their security programs can respond to the changes in the threat environment, but can also leverage the efficiency and effectiveness of unified information security frameworks to assist them in addressing multiple security laws, regulation, and standards.

References

[1] Burrows J. Federal Information Processing Standard (FIPS) PUB 102, Guidelines for computer security certification and accreditation. Maryland: National Institute of Standards and Technology; 1983.

[2] Gallagher P. NCSC-TG-029, Introduction to certification and accreditation. Maryland: National Computer Security Center; 1994.

[3] Gallagher P. NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP). Maryland: National Security Telecommunications and Information Systems Security Committee; 2000.

[4] Money A. DoD 8510.1-M, Department of Defense Information Technology Security Certification and Accreditation Process (DIACAP): application manual. Washington, DC: Department of Defense; 2000.

[5] Ross R, Swanson M, Stoneburnder G, Katzke S, Johnson A. NIST Special Publication (SP) 800-37, Guide for the security certification and accreditation of federal information systems. Maryland: National Institute of Standards and Technology; 2004.

[6] Grimes J. DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP). Washington, DC: Department of Defense; 2007.

[7] McConnell JM. ICD Number 503, Intelligence community information technology system security risk management, certification, and accreditation. Washington, DC: Office of the Director of National Intelligence; 2008.

[8] Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for applying the risk management framework

to federal information systems: a security life cycle approach. Maryland: National Institute of Standards and Technology; 2010.

[9] Shaeffer R. CNSS Instruction No. 4009, National Information Assurance (IA) glossary. Maryland: Committee on National Security Systems; 2010.

[10] Forman M. Guidance to Assist Agencies with Certification and Accreditation. Washington, DC: Executive Office of the President, Office of Management and Budget; 2003.

[11] Valletta A. DoDI 5200.40, DoD Information Assurance Certification and Accreditation Process (DIACAP). Virginia: Department of Defense; 1997.

[12] Grimes J. DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP). Virginia: Department of Defense; 2007.

[13] Wilshusen G. Progress made on harmonizing policies and guidance or national security and non-national security systems. Washington: US Government Accountability Office; 2010.

[14] Takai T. CNSSP No. 22, Policy on information assurance management for national security systems. Maryland: Committee on National Security Systems; 2012.

[15] Public Affairs Office. ODNI News Release No. 08-07, DoD CIO and DNI CIO establish new office to enhance information sharing between DoD and the intelligence community. Washington: Office of the Director of National Intelligence; 2007.

[16] Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-53 Revision 4, Security and privacy controls for federal information systems and organizations (Initial Public Draft). Maryland: National Institute of Standards and Technology; 2012.

[17] Gutierrez C, Jeffrey W. Federal Information Processing Standard (FIPS) PUB 200, Minimum security requirements for federal information and information systems. Maryland: National Institute of Standards and Technology; 2006.

[18] Takai T. Cloud Computing Strategy. Washington: US Department of Defense; 2012.

[19] NIST FISMA Implementation Project [Internet]. Maryland: National Institute of Standards and Technology [cited August 24, 2012] <http://csrc.nist.gov/groups/SMA/fisma/overview.html#phases>.

CHAPTER 8

FedRAMP Primer

INFORMATION IN THIS CHAPTER:

- Introduction to FedRAMP
- FedRAMP Policy Memo
- FedRAMP Concept of Operations
- Third Party Assessment Organization Program

INTRODUCTION TO FEDRAMP

In mid-2009, an inter-agency effort,[1] created under the Federal Cloud Computing Initiative,[2] was established to focus on solving a single problem statement—*How do we best perform security authorization and continuous monitoring for outsourced and multi-agency systems?* [1]. This problem included addressing barriers to the adoption of cloud computing solutions and the cost-effective consolidation of data centers and applications. Traditionally, federal agencies have independently conducted risk management activities through the certification and accreditations (C&As) of their information systems (either residing within the federal agency

[1] The inter-agency effort was conducted within the Cloud Computing Security Working Group that included members from across the government to include: the National Institute of Standards and Technology (NIST), US Department of Defense (DoD), US Department of Education (ED), US Department of Energy (DOE), US Department of Health and Human Services (HHS), US Department of Homeland Security (DHS), US Department of Housing and Urban Development (HUD), US Department of Justice (DOJ), US Department of Labor (DOL), US General Services Administration (GSA), Office of Management and Budget (OMB), Social Security Administration (SSA), and the United States Postal Service (USPS).

[2] From Federal Cloud Computing Initiative (FCCI) [Internet]. Maryland: National Institute of Standards and Technology [cited 2012 Mar 13]. Available from: http://www.info.apps.gov/node/2. *"The Federal Cloud Computing Initiative (FCCI) a part of the Information Technology Infrastructure Line of Business (ITI LoB), is focused on implementing cloud computing solutions for the Federal Government that increase operational efficiencies, optimize common services and solutions across organizational boundaries and enable transparent, collaborative and participatory government."*

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00008-3

accreditation boundary or operated by a contractor on their behalf. Applying this same model to shared services could greatly reduce the overall cost benefit associated with conducting risk management. In addition, there are other issues and challenges associated with applying a singular authorization model such as the incompatibility between different federal agency security policies, differences in acquisition and compliance processes, and an inconsistent and variable application of federal information security and privacy requirements. These issues and challenges are not necessarily new to the federal government, and they existed in the lifecycle of traditional federal IT environments. However, the issues and challenges become more amplified when applied at a larger scale to shared and outsourced information systems, such as a shared services approach which focuses on improving government-wide operational efficiency and effectiveness. Without adopting a more centralized methodology the benefits become less achievable and could potentially inhibit adoption of cloud computing solutions.

The solution—an initiative that would provide joint authorization and continuous security monitoring services using a unified, government-wide risk management approach that federal agencies across the government could leverage [1]. This initiative, known as the Federal Risk and Authorization Management Program (FedRAMP),[3] was designed to focus on three main areas: *authorization*, *continuous monitoring,* and *federal security requirements*. The initial goal of FedRAMP was to establish a unified risk management process that:

- Increased security of cloud solutions through a common assessment approach.
- Eliminated duplication of effort and achieved cost-savings through efficiency.
- Enabled rapid acquisition through leveraged authorizations.
- Improved reuse of authorization packages based on a common set of security requirements.
- Facilitated use of shared services across multiple federal agencies.
- Integrated a government-wide security approach.

In addition to the benefits of unifying under a common risk management framework, commercial service providers also benefited because they only had to perform a single assessment to obtain a provisional authorization to operate (ATO). Since the FedRAMP program also included a single government-wide governance body, federal agencies could leverage the provisional ATOs, greatly reducing their effort because they do not have to individually initiate independent risk management activities.[4]

In November 2010, the FedRAMP PMO released the *Proposed Security Assessment & Authorization for US Government Cloud Computing*. This initial framework was based on 18 months of collaboration with stakeholders across the public and

[3] FedRAMP Program Management Office (PMO). Available from: http://www.fedramp.gov.

[4] Chapter 5 discussed the risk management activities involved in the application of the Risk Management Framework (RMF).

private sector. However, the proposed solution was also developed for the purpose of encouraging a discussion around the "best" approach by gathering "input, knowledge, and experience" [2] necessary for framing the security control requirements and processes for cloud computing environments. The FedRAMP program continued to evolve for the next 13 months until December 8, 2011[5] when the Federal Chief Information Officer (CIO)[6] published a memo titled *Security Authorization of Information Systems in Cloud Computing Environments*, which established the federal policy for the protection of federal information in cloud services. The memo also described the component of the FedRAMP effort, and established milestones for the program and the policy governing the adoption by federal agencies [3].

FEDRAMP POLICY MEMO

The OMB FedRAMP "Policy Memo" established the governing federal policy for the secure adoption and government-wide use of cloud services. The memorandum describes the framework for implementing the FedRAMP components that includes:

- A standard set of security requirements for provisional[7] authorization and ongoing monitoring;
- A conformity assessment program for third-party assessment;
- An assembly of security experts from across government to review authorization documents[8] to support the risk-based decisions by the Joint Authorization Board (JAB)[9];
- Standardized contract language that integrates FedRAMP requirements into the federal government acquisition process, and
- An authoritative central repository for storing authorization documents.

As illustrated in Figure 8.1, the FedRAMP "Policy Memo" is represented at the top of the FedRAMP document hierarchy, providing the highest level of governance. The governance processes defined in the FedRAMP Concept of Operations (CONOPS)

[5] OMB Releases FedRAMP Policy Memo. Available from: http://www.cio.gov/pages.cfm/page/OMB-Releases-FedRAMP-Policy-Memo.

[6] Vivek Kundra, the first US Federal CIO appointed in March 2009, resigned in June 2011, and was replaced by Steven VanRoekel.

[7] From Coleman, C., Spires, R., Takai, T. *Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) Charter Version 1.0.* Washington, DC: FedRAMP Program Management Office, US General Services Administration; 2012. "*A provisional authorization is an initial statement of risk and approval of an authorization package by the JAB pending issuance of a final authorization to operate by the Executive department or agency acquiring the cloud service.*"

[8] Documents included in the authorizing package include: *Security Plan, Security Assessment Report, Plan of Action and Milestones, and Continuous Monitoring Plan.*

[9] As discussed in Chapter 5, Applying the Risk Management Framework, the authorization package includes three key documents, the Security Plan, Security Assessment Report, and the Plan of Action and Milestones. The authorizing official defines additional supporting documents are required.

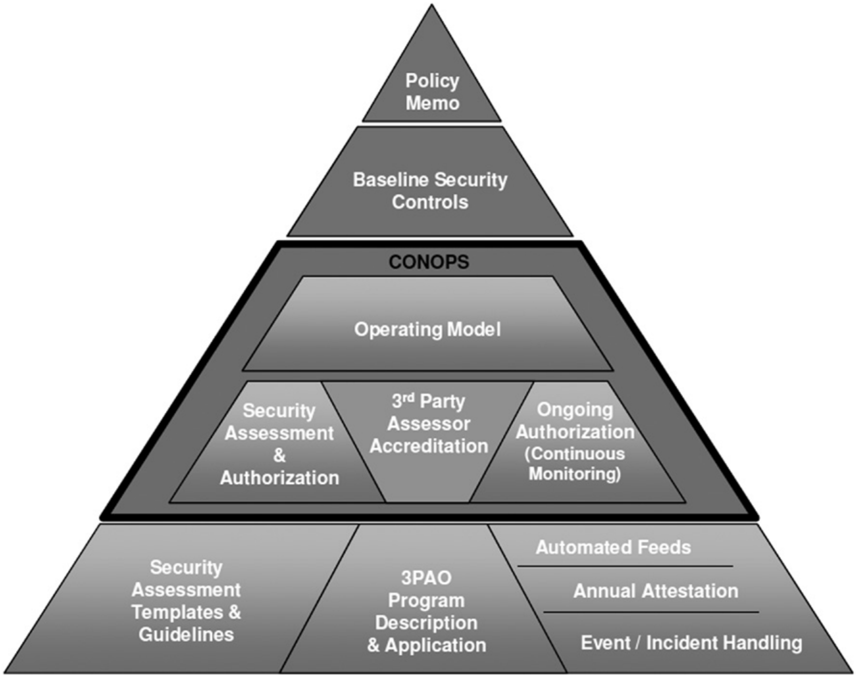

Policy Memo
Baseline Security Controls
CONOPS
Operating Model
Security Assessment & Authorization
3rd Party Assessor Accreditation
Ongoing Authorization (Continuous Monitoring)
Security Assessment Templates & Guidelines
3PAO Program Description & Application
Automated Feeds
Annual Attestation
Event / Incident Handling

FIGURE 8.1 Document Hierarchy [4]

are supported by the foundational elements, which include: (i) security assessment templates and guidelines; (ii) the Third Party Assessment Organization (3PAO) program description and application; and (iii) the three parallel ongoing monitoring mechanisms (*automated/manual data feeds*, *annual attestation*, and *event/incident handling*). The foundational elements provide the FedRAMP PMO with the key functions needed to meet the operating capability for the program.

The scope of coverage for the FedRAMP "Policy Memo" is inclusive of almost all cloud services, regardless of the service and deployment models[10] or whether the cloud service is commercial[11] or non-commercial.[12] In addition, the memo is applied

[10] As defined in NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing*.

[11] From US General Services Administration Federal Acquisition Regulation (FAR) Subpart 2.1 [Internet]. Washington: US General Services Administration [cited 2012 Mar 13]. Available from: https://www.acquisition.gov/far/html/Subpart%202_1.html#wp1145508. *"Commercial item" has multiple requirements as defined in FAR 2.101 such as any item, other than real property, that is of a type customarily used by the general public or by non-governmental entities for purposes other than governmental purposes sold, leased, or licensed to the general public or has been offered for sale, lease or license to the general public.*

[12] Non-commercial includes those products or services that do not fall under the definition of a "commercial item" and are primarily governed by FAR Part 13 ($100,000 and less) and FAR 15 (over $100,000).

government-wide,[13] with the exception of the following conditions in which the requirements under the Federal Information Security Management Act (FISMA)[14] still apply:

- A private cloud[15] deployment model;
- On-premises (i.e., within a Federal facility[16]); and
- Cloud services are not provided to any external entity.[17]

Primary Stakeholders

The four key primary federal government stakeholders for FedRAMP include the US Department of Homeland Security (DHS), the FedRAMP Joint Authorization Board (JAB), the FedRAMP PMO, and the federal agencies. Each of the primary stakeholders shares some responsibility for implementing the FedRAMP "Policy Memo." Figure 8.2 presents a high-level overview of the stakeholders and a workflow that highlights the interactions and relationships existing between each participating Cloud Service Provider (CSP) and 3PAO.

DHS

The DHS National Protection and Programs Directorate (NPPD)[18] includes several divisions, but one specifically, the Office of Cybersecurity and Communications (CS&C), focuses on the "security, resiliency, and reliability of the nation's cyber and communications infrastructure."[19] The CS&C includes the National Cyber Security

[13] From VanRoekel, S. *Office of Management and Budget (OMB) Memorandum, Security Authorization of Information System in Cloud Computing Environments*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. "*This includes Executive departments and agencies not subject to the Federal Acquisition Regulation.*"

[14] FISMA was discussed in detail in Chapter 5, Applying the NIST Risk Management Framework.

[15] From Mell, P., Grance, T. NIST Special Publication (SP) 800-145, The NIST Definition of Cloud Computing. Maryland: National Institute of Standards and Technology; 2011. "*The cloud infrastructure is provisioned for exclusive use by a single organization.*"

[16] From US General Services Administration Federal Acquisition Regulation (FAR) Subpart 2.1 [Internet]. Washington: US General Services Administration [cited 2012 Mar 13]. Available from: https://www.acquisition.gov/far/current/html/Subpart%202_1.html. *Pursuant to 48 C.F.R. 2.101, federally-controlled facilities are buildings or leased space under the jurisdiction, custody or control of a department or agency, including those spaces included in commercial buildings shared with non-government tenants and/or contractor-operated under a management and operating contract.*

[17] From VanRoekel, S. *Office of Management and Budget (OMB) Memorandum, Security Authorization of Information System in Cloud Computing Environments*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. *External entities, depending on where in the federal government hierarchy the cloud service is deployed, includes external users and could include bureaus, components, or subordinate organizations within a federal agency.*

[18] *National Protection and Programs Directorate (NPPD)*. Available from: http://www.dhs.gov/about-national-protection-and-programs-directorate.

[19] *Office of Cybersecurity and Communications (CS&C)*. Available from: http://www.dhs.gov/office-cybersecurity-and-communications.

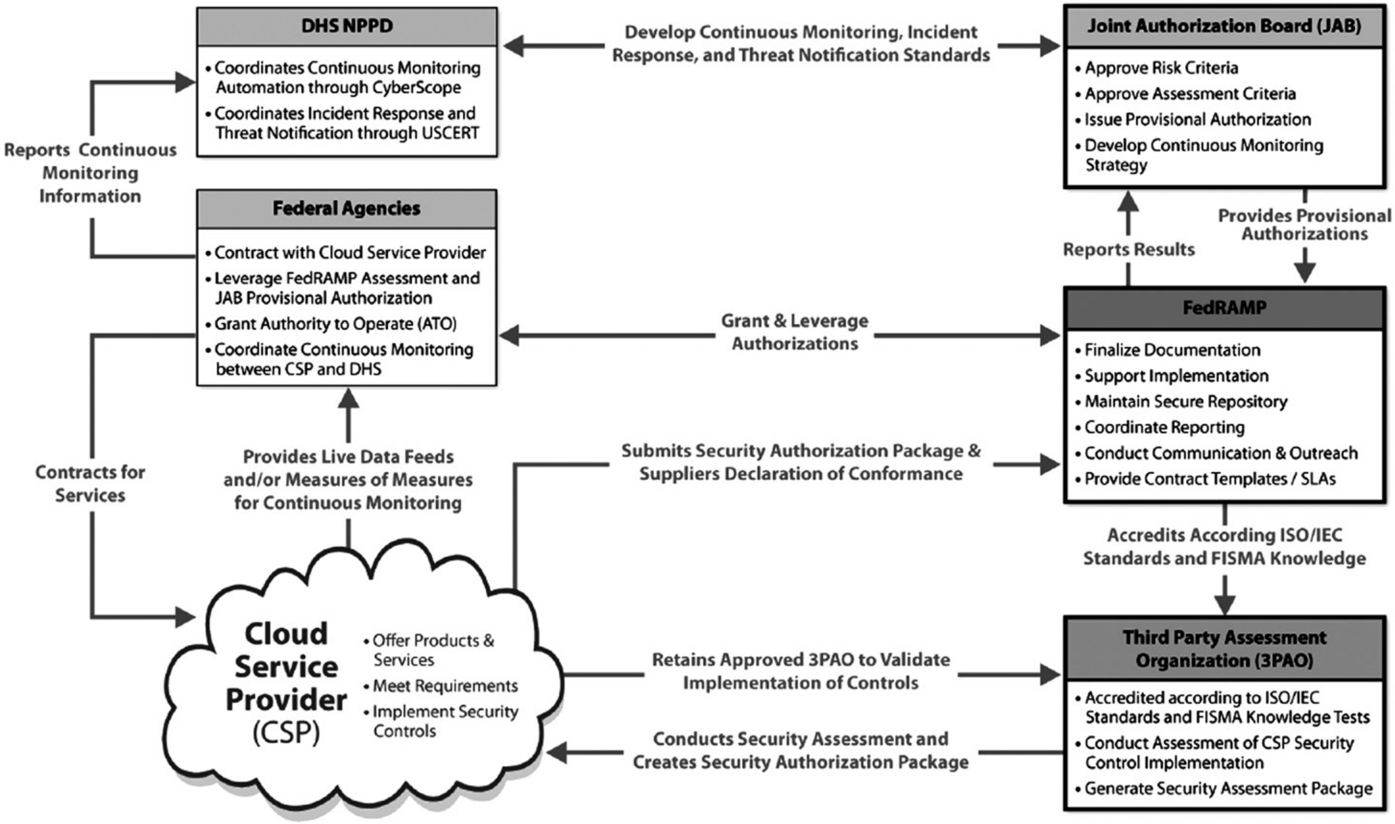

DHS NPPD
• Coordinates Continuous Monitoring Automation through CyberScope
• Coordinates Incident Response and Threat Notification through USCERT
Develop Continuous Monitoring, Incident Response, and Threat Notification Standards
Joint Authorization Board (JAB)
• Approve Risk Criteria
• Approve Assessment Criteria
• Issue Provisional Authorization
• Develop Continuous Monitoring Strategy
Reports Continuous Monitoring Information
Federal Agencies
• Contract with Cloud Service Provider
• Leverage FedRAMP Assessment and JAB Provisional Authorization
• Grant Authority to Operate (ATO)
• Coordinate Continuous Monitoring between CSP and DHS
Reports Results
Provides Provisional Authorizations
Grant & Leverage Authorizations
FedRAMP
• Finalize Documentation
• Support Implementation
• Maintain Secure Repository
• Coordinate Reporting
• Conduct Communication & Outreach
• Provide Contract Templates / SLAs
Contracts for Services
Provides Live Data Feeds and/or Measures of Measures for Continuous Monitoring
Submits Security Authorization Package & Suppliers Declaration of Conformance
Accredits According ISO/IEC Standards and FISMA Knowledge
Cloud Service Provider (CSP)
• Offer Products & Services
• Meet Requirements
• Implement Security Controls
Retains Approved 3PAO to Validate Implementation of Controls
Conducts Security Assessment and Creates Security Authorization Package
Third Party Assessment Organization (3PAO)
• Accredited according to ISO/IEC Standards and FISMA Knowledge Tests
• Conduct Assessment of CSP Security Control Implementation
• Generate Security Assessment Package

FIGURE 8.2 FedRAMP Stakeholder Roles and Interactions [4]

Division (NCSD),[20] which has the primary objective of protecting and securing cyberspace and cyber assets, and includes a function specifically focusing on the security of federal networks.

In July 2010, through the Director of OMB, the Special Assistant to the President and Cybersecurity Coordinator, published OMB Memorandum 10-28[21] to clarify the cybersecurity responsibilities and activities. This memo set out the lines of responsibility and authority to reduce overlap and ensure the cost-effective application of resources needed for the government-wide coordination of cybersecurity efforts. In addition, the memo aligned cybersecurity-related roles and responsibilities (see (a)), including limitations (see (b) and (c)) for the implementation of FISMA[22]:

- Section 3543(a)—The Director of OMB "shall oversee agency information security policies and practices, including developing and overseeing the implementation of policies, principles, standards, and guidelines on information security" [5].
- Section 3543(b) and (c)—Limitations associated with National Security Systems (NSSs) and Department of Defense (DoD) and Intelligence Community (IC) information systems.

The responsibilities assigned under this memo were inherited by the FedRAMP "Policy Memo" and gave the DHS the responsibility under FedRAMP for four key areas:

- Government-wide and agency-specific cybersecurity assistance;
- Cybersecurity operations and incident response coordination;
- Continuous monitoring standards development[23];
- Trusted Internet Connection (TIC) program implementation.[24]

JAB

The JAB was chartered under a joint agreement[25] between the Chief Information Officers (CIOs) of GSA, DHS, and DoD with the objective of:

- Defining and regularly reviewing the security authorization requirements;
- Approving accreditation criteria for the Third Party Assessment Organizations (3PAOs);

[20] Functions within the NCSD include the national cyberspace response system which seeks to protect the national cyber infrastructure, the federal network security branch, and cyber risk management programs.

[21] Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and Department of Homeland Security. Available from: http://www.whitehouse.gov/omb/assets/memoranda.../m10-28.pdf.

[22] FISMA was discussed in detail in Chapter 5, Applying the NIST Risk Management Framework.

[23] In September 2010, the DHS Federal Network Security branch published the Continuous Asset Evaluation, Situational Awareness and Risk Scoring (CAESARS) architectural reference framework which has been adopted by NIST through Interagency Reports as an Enterprise Continuous Monitoring Reference Model (also known as the CAESARS Framework Extension).

[24] The TIC program was original published as an OMB Initiative in Office of Management and Budget (OMB) Memorandum 08-05 with the focus of optimizing federal network services into a common solution for the federal government.

[25] *FedRAMP JAB Charter*. Available from: http://www.gsa.gov/graphics/staffoffices/FedRAMP_JAB_Charter_SIGNED.pdf.

- Establishing the criteria for the queue that will prioritize authorization package review;
- Reviewing authorization packages;
- Granting provisional authorizations;
- Ensuring reviews and updates of provisional authorization;
- Establishing mechanisms for the maintenance of the security authorization requirements.

The JAB is comprised of Authorizing Officials (AOs) and AO-designated technical representatives from GSA, DHS, and DoD, and is supported through the FedRAMP PMO that operates within the GSA, Office of Citizens Services and Innovative Technologies (OCSIT).

FedRAMP PMO

The FedRAMP PMO is a critical operational function that provides most of the administrative and technical support for FedRAMP processes and frameworks,[26] to include facilitating the implementation of the assessment and authorization (A&A) processes in the NIST RMF,[27] excluding the actual authorization. In addition, the FedRAMP PMO operates most of the programmatic functions of the FedRAMP processes and activities that support the key components included in Figure 8.1 of the FedRAMP operating model such as:

- 3PAO conformity assessment program.
- Authorization package queue.
- Education and outreach.
- Authorization repository.
- Security assessment templates and guidelines, to include Memorandums of Understanding (MOUs)/Memorandums of Agreement (MOAs) and standard contract language and Service Level Agreements (SLAs).

Federal Agencies

The role of the federal agency in FedRAMP is as a federal customer which uses the processes (e.g., CONOPS, NIST RMF, etc.), and documentation (e.g., FedRAMP templates, NIST standards and guidelines, FedRAMP authorization packages, etc.) to procure and use cloud services to meet the objectives of the "Cloud First" policy, originally discussed in the *25 Point Implementation Plan to Reform Federal Information Technology Management* [28] and further defined in the *Federal Cloud Computing Strategy.* [29]

[26] (a) Security and privacy requirements harmonization, (b) federal agency guidance, (c) security authorization initiation requests, (d) authorization package leveraging, and (e) continuous monitoring.

[27] NIST RMF was discussed in detail in Chapter 5, Applying the NIST Risk Management Framework.

[28] *25 Point Implementation Plan to Reform Federal Information Technology Management*. Available from: http://cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf.

[29] *Federal Cloud Computing Strategy*. Available from: http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf.

NOTE

The FedRAMP process provides a structured approach for use by the federal government. The FedRAMP process also offers a catalyst for developing similar processes and practices that will be used by the private sector when adopting cloud services. By offering a similar model for conducting due diligence when evaluating the information security, risk management, and compliance of cloud services, the Cloud Security Alliance (CSA) developed the Open Certification Framework (OCF), a program for flexible, incremental, and multi-layered cloud provider certification according to the CSA's industry-leading security guidance and control objectives. The FedRAMP operates under a "do once, use many times" concept, where the CSA OCF operates under a "certify-once, use-often" concept. However, both models can also be used as options by cloud service providers, saving both time and cost associated with consumer due diligence activities. In addition, by leveraging cloud services that have been reviewed under the FedRAMP and OCF model, cloud consumers can reduce the need to perform their own due diligence, potentially accelerating the development and deployment of new products and services.

The federal agency, as a party within a contract[30] for cloud services, is to use FedRAMP as a cost-effective mechanism for the secure adoption of cloud services that are within the scope of the FedRAMP "Policy Memo."

FEDRAMP CONCEPT OF OPERATIONS

The initial version of the FedRAMP Concept of Operations (CONOPS) was published on February 7, 2012. The CONOPS leveraged the initial draft of the FedRAMP A&A processes[31] and similarly included: *security assessment*, *security authorization,* and *continuous monitoring*. However, through the maturity of the program, the initial processes were expanded to address those core process elements that will be governed by FedRAMP to support several important outputs:

- Adequacy of information security for cloud services.
- Implementation of a common risk management approach.
- Improved procurement of cloud services.

As previously illustrated in Figure 8.2, FedRAMP requires the interaction of multiple participants. The FedRAMP CONOPS further elaborated on the role of each participant in Table 8.1.

[30] Cloud services can be a "public cloud" or a federal "community cloud" that provides shared services. For example, the Bureau of the Public Debt, Administrative Resource Center (BPD-ARC), a part of the US Treasury, provides Government-to-Government Shared Services that provides services leveraged by other federal agencies. For more information on the BPD-ARC, visit: https://arc.publicdebt.treas.gov/.

[31] Proposed Security Assessment & Authorization for US Government Cloud Computing. Available from: https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf.

Table 8.1 Major FedRAMP Participants

Participant	Role and Responsibility
Federal Agency Customer (or Contractor operating on behalf of a Federal Agency)	The Cloud Consumer for a cloud service that will be used to store, process, or transmit federal information is required to follow the FedRAMP process as part of the acquisition process.
Cloud Service Provider (CSP)	The Cloud Provider that will be providing the cloud service to a federal agency (or contractor operating on behalf of a federal agency) is required to meet the FedRAMP security requirements and agency-specific requirements (where applicable).
Third Party Assessment Organization (3PAO)	The Cloud Auditor that will be providing the independent assessment of cloud service is required to validate and attest to the quality and compliance of the CSP based on its security authorization package.
Joint Authorization Board (JAB)	The JAB is the authorizing body that reviews the security authorization package and grants provisional authority to operate (ATO).
FedRAMP Program Management Office (PMO)	The FedRAMP PMO is a program management function that manages the security assessment, authorization, and continuous monitoring processes.

The FedRAMP CONOPS provides the high-level overview and operating model that encompasses three key process areas that govern the life cycle of a cloud computing service within FedRAMP. As shown in Figure 8.3, the FedRAMP operational capability focuses on processes that include: *conducting security assessments, leveraging of provisional authorizations,* and *continuous monitoring*. To support the operational capability the FedRAMP CONOPS describes the relationship between the document hierarchy in Figure 8.1 and a structured application of the processes (i.e., the relationship between the conceptual operation of FedRAMP and the various roles and responsibilities within each of the processes).

Operational Processes

FISMA requires federal agencies to ensure the protection of federal information and information systems. The accountability for this requirement cannot be transferred to the FedRAMP PMO, but instead, as illustrated in Figure 8.2, it is shared between the FedRAMP PMO and the federal agency based on the scope of the evaluation (i.e., FedRAMP security requirements baseline vs. the agency-specific security and privacy requirements). The FedRAMP processes used in conducting the A&A of cloud services are designed to be compatible with the existing risk management practices already defined by NIST and used in traditional IT environments or FedRAMP-exempt cloud solutions. Therefore, only the differences within the FedRAMP processes and the NIST RMF[32] will be discussed in this section.

[32] NIST RMF was discussed in detail in Chapter 5, Applying the NIST Risk Management Framework.

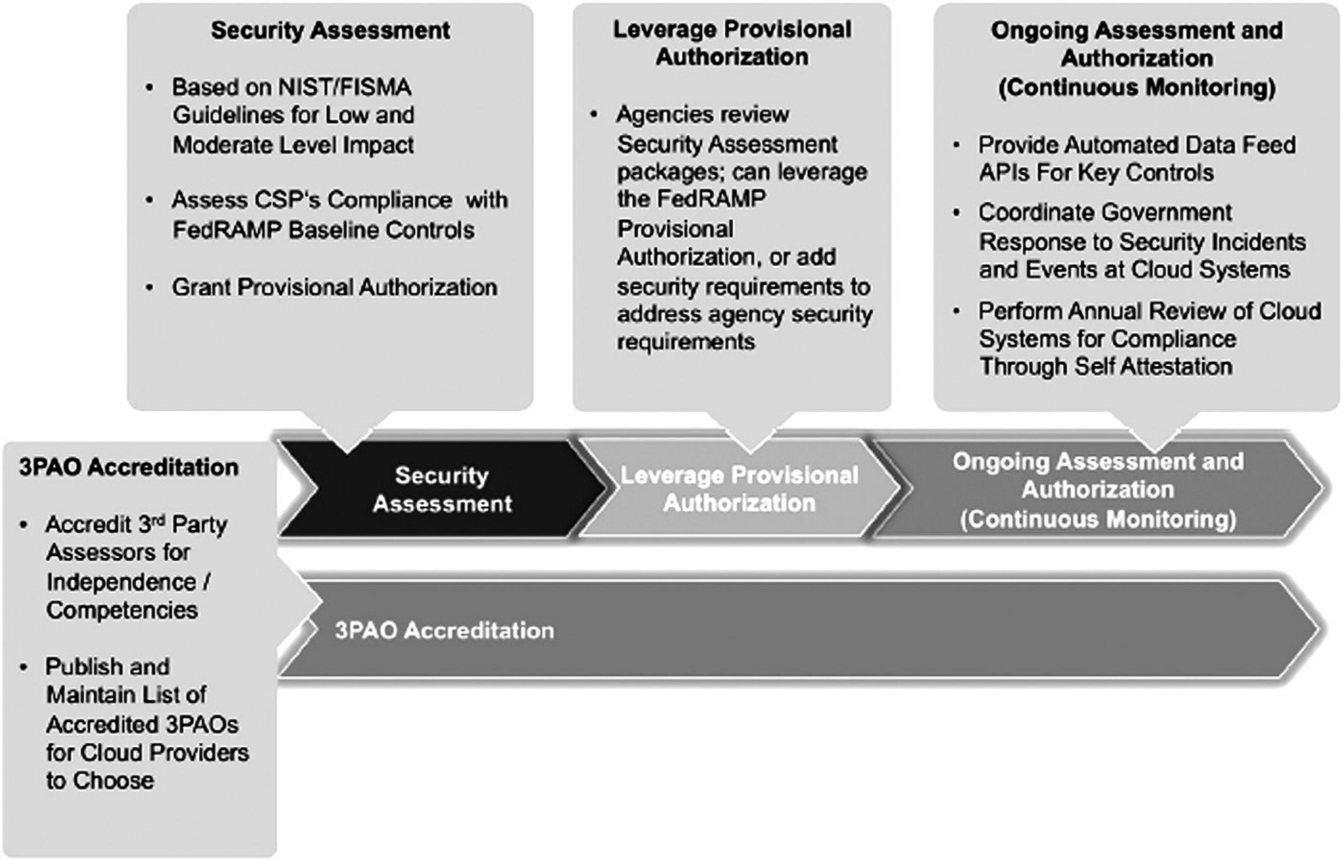

Security Assessment
• Based on NIST/FISMA Guidelines for Low and Moderate Level Impact
• Assess CSP's Compliance with FedRAMP Baseline Controls
• Grant Provisional Authorization
Leverage Provisional Authorization
• Agencies review Security Assessment packages; can leverage the FedRAMP Provisional Authorization, or add security requirements to address agency security requirements
Ongoing Assessment and Authorization (Continuous Monitoring)
• Provide Automated Data Feed APIs For Key Controls
• Coordinate Government Response to Security Incidents and Events at Cloud Systems
• Perform Annual Review of Cloud Systems for Compliance Through Self Attestation
3PAO Accreditation
• Accredit 3rd Party Assessors for Independence / Competencies
• Publish and Maintain List of Accredited 3PAOs for Cloud Providers to Choose
Security Assessment
Leverage Provisional Authorization
Ongoing Assessment and Authorization (Continuous Monitoring)
3PAO Accreditation

FIGURE 8.3 FedRAMP Process Areas [6]

Security Assessment Process

The FedRAMP JAB, in collaboration with the Federal CIO Council and Federal Chief Information Security Officer (CISO) community, defined two additional sets of security control baselines that extend the existing NIST security control baselines[33] for *Low-* and *Moderate-Impact* cloud-based information systems. As will be discussed in more detail in Chapter 9, these minimum security controls have been tailored and supplemented to establish a standardized set of security requirements considered to provide adequate protection for federal information within cloud computing environments. In addition to the initial tailoring of the NIST security control baselines by the JAB (i.e., applying the *scoping guidance* and specifying government-wide *organization-defined parameters*), CSPs also have the responsibility for completing additional tailoring for the application of security controls that may differ from the FedRAMP security control requirements (i.e., specifying *compensating security controls*). For example, in Table 8.2, the security controls selection process (NIST RMF Step 2) maps to two additional FedRAMP deliverables: *Control Tailoring Workbook (CTW)* and *Control Implementation Summary (CIS)*. The CTW is used by the CSPs to document their "control implementation and define their implementation settings for FedRAMP defined parameters and any compensating controls" [6]. The CIS is used by the CSP to summarize the control ownership and indicate which controls are owned and managed by the CSP and which are owned and managed by the leveraging federal agency.

Initiating a Request

The first process area of the FedRAMP security assessment process, initiating a request,[34] involves the definition of the scope of the cloud service. The four steps included in Table 8.2 provide a mapping to similar types of steps performed within the NIST RMF as applied by federal agencies for traditional IT environments or FedRAMP-exempt information systems. In addition, this process area applies specific adaptations of the NIST RMF for the purpose of enabling a more programmatic interaction when performing the risk management activities; however, the intent of the NIST-defined processes are maintained.

Identified below are the outputs from the steps included within the security assessment control process area when initiating a request:

Major Milestone Outputs:

- Categorization of the cloud service, including the information to be processed, stored, or transmitted.

[33] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation."*

[34] The FedRAMP initiation can be performed by both the sponsoring federal agency and the CSP. Available from: http://www.gsa.gov/portal/content/125991.

Table 8.2 NIST RMF and FedRAMP 1.1 Process Area/Deliverables

FedRAMP Process Area	FedRAMP Deliverables	NIST RMF Step
1.1—Initiate Request • *Step 1*—Document Service Boundary and Assets • *Step 2*—Identify Impact Level • *Step 3*—Tailor Controls • *Step 4*—Define Control Implementations	• FedRAMP Request Form (CSP or Federal Agency)[a] • FIPS 199 Categorization[b]	RMF Step 1—Categorize Information System • *Task 1.1*—Security Categorization • *Task 1.2*—Information System Description • *Task 1.2*—Information System Registration
	• Control Tailoring Workbook (CTW)[c] • Control Implementation Summary (CIS)[d]	RMF Step 2—Select Security Controls • *Task 2.1*—Common Control Identification • *Task 2.2*—Security Control Selection • *Task 2.3*—Monitoring Strategy • *Task 2.4*—Security Plan Approval

[a] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Used by Federal Agencies and CSPs to request initiation of the FedRAMP security assessment process."*

[b] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Used to determine the impact level to be supported by the cloud information system/service."*

[c] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Used by the CSP to document their control implementation and define their implementation settings for FedRAMP defind parameters and any compensating controls."*

[d] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Summarizes the control ownership and indicates which controls are owned and managed by the CSP and which controls are owned and managed by the leveraging agency."*

- Registration of the cloud service with the FedRAMP PMO.
- Allocation of security controls to the cloud service as system-specific or any controls inherited as hybrid (*partially*) or common (*completely*).
- Identification of control responsibility between the CSP and the federal government.
- Approval of the tailored and supplemented baseline security controls as allocated and described in the CTW and the CIS.

Documenting the Security Controls

Documenting security controls, described in Table 8.3, maps to the corresponding NIST RMF Step 3 (*Implement Security Controls*). In this process area, the CSP implements the required security controls and documents the implementation in the System Security Plan (SSP). The SSP provides the JAB with the necessary visibility through the functional descriptions of how the security controls have been integrated into the cloud service and the operating environment. "The functional description of the security control implementation includes *planned inputs, expected behavior, and expected outputs* where appropriate, typically for those technical controls that are employed in the hardware, software, or firmware components of the information system" [7]. The SSP describes the controls implemented, and also provides a method for communicating to the JAB those security controls which have been planned or compensated by the CSP.

Before the security control implementations can be described, the CSP needs to identify the information system components included within the operating environment. Since cloud environments can be configured differently and encompass different layers (e.g., a single provider operates the IaaS layer, a single or different provider operates the IaaS and PaaS layers, or a single provider operates all layers or only the SaaS layer), it is important for the CSP to accurately reflect the security control boundary layer to ensure gaps do not exist between each layer.

Identified below are the outputs from the steps included within the security assessment control process area when documenting security controls.

Major Milestone Outputs:

- Documentation of the security controls implemented in the cloud service as included within the approved baseline security controls allocated and described in the CTW and the CIS.

TIP

The FedRAMP PMO identified the following list of questions [13] to assist CSPs in describing the scope of the boundary for their cloud service. Below is a subset of those questions:

- Does the cloud service leverage an existing Provisional Authorization?
- Do tenants share the same VLAN(s)?
- Are virtual machine zones isolated on unique network segments?
- Are separate physical network adapters used to isolate virtual machine zones?
- Is layer-2 isolation performed?
- Are firewalls used to provide isolation between tenants?
- Are router ACLs used to provide isolation between tenants?
- Are network zones used, and if so, how are those zones defined?
- Do you have the capability to identify the geographic location where the customer data is stored?
- Do you have the capability for a federal agency customer to identify the geographic location where its data are stored?
- Is live migration used, and if so, is it performed manually or automatically?
- If live migration is automated, what rules are used to govern the migration?

Table 8.3 NIST RMF and FedRAMP 1.2 Process Area/Deliverables

FedRAMP Process Area	FedRAMP Deliverables	NIST RMF Step
1.2—Document Security Controls • *Step 1*—Document System Security Plans	• System Security Plan (SSP)[a] • Information Security Policies[b] • User Guide[c] • Rules of Behavior (RoB)[d] • IT Contingency Plan (CP)[e] • Configuration Management Plan (CM)[f] • Incident Response Plan (IRP)[g] • E-Authentication Workbook[h] • Privacy Threshold Analysis (PTA)[i] • Privacy Impact Assessment (PIA)[j]	RMF Step 3—Implement Security Controls • *Task 3.1*—Security Control Implementation • *Task 3.2*—Security Control Documentation

[a] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Describe how the controls are implemented within the cloud information system and its environment of operation."*

[b] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Describes the CSPs Information Security Policy that governs the system described in the SSP."*

[c] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Describes how the leveraging agencies use the system."*

[d] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Used to define the rules that describe the system user's responsibilities and expected behavior with regard to information and information usage and access."*

[e] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Used to define and test interim measures to recover information system services after a disruption."*

[f] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Describes how changes to the system are managed and tracked."*

[g] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Documents how incidents are detected, reported, and escalated and should include timeframes, points of contact, and how incidents are handled and remediated."*

[h] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Used to indicated if E-Authentication will be used in the cloud system and defines the required authentication level (1–4) in terms of consequences of the authentication errors and misuse of credentials."*

[i] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Used to help determine if a Privacy Impact Assessment is required."*

[j] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Assess what Personally Identified Information (PII) is captured and if it is being properly safeguarded."*

Performing the Security Assessment

In this step of the security assessment process area, as outlined in Table 8.4, the CSP works directly with a contracted accredited[35] Third Party Assessment Organization (3PAO). The 3PAO is responsible for performing an independent and qualified assessment of the security controls using the artifacts included in the security assessment package. The assessment-related activities performed in this step are consistent with those included within the NIST RMF Step 4 and involve a collaborative relationship between the CSP and the 3PAO to ensure assessor independence is maintained. The output of this task involves making a determination of the extent to which the controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the FedRAMP security requirements [7].

In addition to the assessment activities included in NIST RMF Step 4, the CSP also has responsibility in documenting a remediation plan (or plan of action and milestones (POA&Ms)),[36] which is performed in NIST RMF Step 5. After reviewing the security assessment report (SAR) generated by the 3PAO, the CSP is required to prepare POA&Ms[37] that require establishing the tasks, resources required to complete the task, and the schedule for remediating any findings of weaknesses and deficiencies. The 3PAO SAR and the POA&Ms are two of the three key documents in the security authorization package submitted and reviewed by the JAB when making a risk-based decision for granting a Provisional Authorization.

Identified below are the outputs from the steps included within the security assessment control process area when performing the security assessment.

Major Milestone Outputs:

- Approved security assessment plan used to assess the security control employed within or inherited by the cloud service.
- SAR that identifies the findings and recommendations based on an assessment of the security controls implemented within the cloud service.
- POA&Ms that include remediation action for correcting weaknesses and deficiencies in the cloud service.

[35] List of accredited 3PAOs can be found at FedRAMP.gov. Available from: http://www.gsa.gov/portal/content/131991.

[36] From FedRAMP Program Management Office (PMO), FedRAMP Plan of Action and Milestones Template. Washington: US General Services Administration; 2012. "*The plan of action and milestones (POA&M) is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system.*"

[37] From FedRAMP Program Management Office (PMO), FedRAMP Plan of Action and Milestones Template. Washington: US General Services Administration; 2012. "*All High and Moderate findings from the Security Assessment Report should be mapped into the POA&M. High impact vulnerability needs to be mitigated within 30 days, and Moderate impact vulnerabilities need to be mitigated within 90 days.*"

Table 8.4 NIST RMF and FedRAMP 1.3 Process Area/Deliverables

FedRAMP Process Area	FedRAMP Deliverable	NIST RMF Step
1.3—Performing the Security Assessment • *Step 1*—Develop Testing Plan • *Step 2*—Audit Control Implementations • *Step 3*—Perform Vulnerability/ Penetration Testing	• 3PAO Designation Form[a] • Security Assessment Plan (SAP)[b] • Security Assessment Test Cases[c] • Security Assessment Report (SAR)[d]	RMF Step 4—Assess Security Controls • *Task 4.1*—Assessment Preparation • *Task 4.2*—Security Control Assessment • *Task 4.3*—Security Assessment Report • *Task 4.4*—Remediation Actions
• *Step 4*—Develop Plan of Action and Milestones (POA&Ms)	• Plan of Action and Milestones (POA&Ms)[e]	RMF Step 5—Authorize Information System • *Task 5.1*—Plan of Action and Milestones

[a] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "CSP submits this form to FedRAMP in order to designate the FedRAMP accredited 3PAO that will perform an independent assess of the CSPs system."*

[b] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Describes CSPs specific tasks and timelines for remediating or changing system or control specific implementations."*

[c] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Based on NIST SP 800-53A."*

[d] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Used to document the overall status and deficiencies in the security controls."*

[e] *From FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. "Describes the scope of the assessment."*

Finalizing the Security Assessment

The final step in the security assessment process area, as outlined in Table 8.5, is the assembly of the documentation by the CSP into a security authorization package that includes the Supplier's Declaration of Conformation.[38] The JAB reviews the security authorization package and makes the final risk-based decision when granting a Provisional Authorization. This risk determination is based on an accumulation of risk-related information that is used by the JAB when assessing the risk to the federal government when using the cloud service.

[38] From Global Standards Information, Supplier's Declaration of Conformity [Internet]. Maryland: National Institute of Standards and Technology [cited 2012 Mar 22]. Available from: http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-208. *"A Supplier's Declaration of Conformity (SDOC) is a first party assessment in which a supplier or manufacturer provides written assurance of conformity."*

Table 8.5 NIST RMF and FedRAMP 1.4 Process Area/Deliverables

FedRAMP Process Area	FedRAMP Deliverable	NIST RMF Step
1.4—Finalizing the Security Assessment • *Step 1*—Compile All Updated and Final Documentation • *Step 2*—Answer Questions from Final Risk Assessment • *Step 3*—Accept the Documented Findings and Make Any Updated to POA&Ms • *Step 4*—Accept Provisional Authorization	• Finalized Security Assessment Package[a] • Supplier's Declaration of Conformity (SDOC)[b]	RMF Step 5—Authorize Information System • *Task 5.2*—Security Authorization Package • *Task 5.3*—Risk Determination • *Task 5.4*—Risk Acceptance

[a] *"Complete package of all security assessment deliverables and related evidence."*

[b] *From Global Standards Information, Supplier's Declaration of Conformity [Internet]. Maryland: National Institute of Standards and Technology [cited 2012 Mar 22]. Available from: http://gsi.nist.gov/global/index.cfm/L1-5/L2-45/A-208. "CSPs verify and attest to the trust of the implemented security controls as detailed in their assessment package."*

Identified below are the outputs from the steps included within the security assessment control process area when finalizing the security assessment:

Major Milestone Output:

- Security assessment package that includes the key documents used in making an authorization decision—the SSP, SAR, and POA&Ms.
- Provisional ATO letter that includes the risk determination and acceptance decision by the JAB for cloud service.

Leveraging the ATO

Leveraging is an authorization approach,[39] previously discussed in Chapter 5, which is used when one federal agency accepts the authorization package of another federal agency. The leveraging federal agency's AO reviews and accepts the risk based on a determination of the risk for using the cloud service to support their specific mission and business processes and use the cloud service to store,

[39] Three authorization approaches are available by AOs when conducting authorizations: (1) traditional single AO ATO, (2) multiple AO ATO, and (3) leveraged ATO.

process, or transmit their information. In this FedRAMP process area, the final acceptance of risk (or ATO) is granted by the leveraging federal agency[40] accepting the provisional ATO for cloud service. This includes the agreement of the control responsibility as allocated by the CSPs in the CIS, as discussed earlier in this chapter.

Continuous Monitoring

In the final process area, ongoing assessment and authorization (also known as continuous monitoring), the JAB determines if the security controls implemented are still effective and the Provisional Authorization should be maintained.[41] This determination is based on three keys areas: *operational visibility, change control process,* and *incident response*. The operational visibility focuses on periodic assessment of a select subset of security controls to ensure security controls implemented by CSPs continue to be effective. The change control process relates to the CSPs' ability to understand security impacts associated with changes to the cloud service. Incident response focuses on identifying new threats and vulnerabilities and the response and mitigate activities for incidences. Continuous monitoring will be discussed in detail in later chapters. However, in this section, a high-level overview will be provided as it relates to the FedRAMP CONOPS.

Operational Visibility

Operational visibility focuses on three sources of information for determining the security and risk posture of cloud services to demonstrate continued compliance through the automation to enable oversight and monitoring. Originally included in the reporting instructions[42] to federal agencies in April 2010, a three-tiered approach[43] was introduced as a method for federal agencies to effectively and

[40] There are four types of security assessment package categories that will be maintained in the FedRAMP repository.

[41] From FedRAMP Program Management Office (PMO), Continuous Monitoring Strategy & Guide. Washington: US General Services Administration; 2012. "*To receive reauthorization of a FedRAMP Provisional Authorization from year to year, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable*."

[42] Office of Management and Budget (OMB) Memorandum 10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. Available from: www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf.

[43] From Zients, J., Kundra, V., Schmidt, H. *Office of Management and Budget (OMB) Memorandum 10-15, FY 2010 Reporting Instructions for the Federal Information System Management Act and Agency Privacy Management*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010. *"The three-tiered approached is a result of the task force established in September 2009 to develop new, outcome-focused metrics for information security performance for Federal agencies."*

"continuously monitor security-related information across the enterprise in a manageable and actionable way" [8]. To enable near-real-time monitoring, Cyber-Scope was introduced as the platform for submitting data feeds (automated and manual) and to enable OMB and DHS[44] to conduct government-wide benchmarking through a set of questions/metrics[45] that describe each on the federal agencies' security posture.

As part of the continuous monitoring requirements, CSPs are required to submit similar types of data elements to federal agencies to use in meeting their reporting requirements and to give the FedRAMP PMO operational visibility into the security posture of cloud services. In addition, CSPs are required to conduct an annual re-assessment of a subset of the security controls identified in the FedRAMP baseline and submit an annual self-attestation report.

Change Control

Changes to an operational environment are inevitable as a system undergoes routine maintenance. However, some changes may cause significant impacts to the security posture of the cloud service.[46] Therefore, the CSP is required to report "changes in the CSP's point of contact with FedRAMP, changes in the CSP's risk posture, changes to any applications residing on the cloud system, and/or changes to the cloud system infrastructure" [6], and submit any residual artifacts associated with significant changes such as the SSP, security impacts analysis, and a re-assessment by a 3PAO to the FedRAMP PMO.

Incident Response

Incident response plans ensure there is bi-lateral communication on incidents between the CSP and the federal government. Depending on the type of incident and the scope of the impact, a single incident could impact multiple federal agencies leveraging the cloud service [9]. The notification of incidents and coordination with the United States Computer Emergency Readiness Team (US-CERT)[47] and federal agency Security Operations Centers (SOCs) ensures there is a managed response and escalation of incidences.

[44] In July 2010 through the responsibilities outlined in OMB Memorandum 10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security,* DHS was given the primary responsibility for operational aspects of cybersecurity with respect to the federal information system covered under FISMA as defined in Section 3545.

[45] In February 2012, DHS published the *FY 2012 Chief Information Officer Federal Information Security Management Act Reporting Metrics, which* requires federal agencies to report on cloud services. Available from: http://www.dhs.gov/xlibrary/assets/nppd/ciofismametricsfinal.pdf.

[46] Depending on the cloud service and deployment model, changes to the cloud service could affect other services or applications within the cloud stack.

[47] *US-CERT*. Available from: http://www.us-cert.gov.

THIRD PARTY ASSESSMENT ORGANIZATION PROGRAM

Conformity assessments[48] are not new to the federal government. As discussed in Chapter 2, the federal government has a role in supporting standards development.[49] For example, NIST,[50] which chairs the Interagency Committee on Standards Policy (ISCP),[51] has the responsibility[52] of coordinating public and private sector standards and conformity assessment activities. In the 3PAO Program, the FedRAMP PMO in coordination with NIST designed "a conformity assessment process for use with FedRAMP to ensure the independence of and the management and the technical quality of 3PAOs uses a standard and consistent security assessment process" [10]. The conformity assessment process[53] gives the federal government the confidence of the security in using cloud services through:

- the conformance with an established set of security standards and requirements;
- a consistently applied security assessment process; and
- the use of a structured approach when granting provisional ATOs.

In the FedRAMP process, the 3PAO[54] plays a critical role in providing the FedRAMP JAB with an independent evaluation (or inspection[55]) to ensure the cloud

[48] From Global Standards Information, Federal Register, Vol. 65, No. 155, Guidance on Federal Conformity Assessment Activities. Maryland: National Institute of Standards and Technology; 2000. *"Conformity assessment means any activity concerned with determining directly or indirectly that requirements are fulfilled."*

[49] Office of Management and Budget (OMB) Circular No A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*. Available from: http://www.whitehouse.gov/omb/circulars_a119.

[50] NIST, a US government's standards agency, collaborates with other standards development organizations (SDOs) such as the American National Standards Institute (ANSI), which is the representative for the United States in the International Organization for Standards (ISO).

[51] *Interagency Committee on Standards Policy (ICSP)*. http://standards.gov/icsp/query/index.cfm.

[52] Reference Section 12 of the *National Technology Transfer and Advancement Act (NTAA) of 1995*. Available from: http://standards.gov/nttaa.cfm.

[53] ISO/IEC 17020:1998, General Criteria for the operation of various types of bodies performing inspection. ISO/IEC 17020:1998 has been withdrawn and replaced by the revised version ISO/ IEC 17020:2012, Conformity assessment—Requirements for the operation of various types of bodies performing inspection—http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=52994.

[54] From FedRAMP Program Management Office (PMO). General FedRAMP FAQ [Internet]. Washington: US General Services Administration [cited 2011 Mar 15]. Available from: http://www.gsa.gov/portal/content/118887. *"Third Party Assessment Organizations (3PAOs) perform initial and ongoing independent verification and validation of the security controls deployed within the Cloud Service Provider's information system."*

[55] From Global Standards Information, Federal Register, Vol. 65, No. 155, Guidance on Federal Conformity Assessment Activities. Maryland: National Institute of Standards and Technology; 2000. *"Inspection is defined as the evaluation by observation and judgment accompanied as appropriate by measurement, testing or gauging of the conformity of a product, process or service to specified requirements."*

TIP

Independent assessors or assessment teams must be capable of conducting an impartial assessment. What qualifies an assessor or assessment team as being capable of presenting results in a manner that would enable the Joint Authorization Board (JAB) in making a "credible, risk-based decision" is determined through the Third Party Assessment Organization (3PAO) Program. In addition to the 3PAO program, "CSPs should establish minimum personnel requirements such as the CCSK with other credentials like the CISSP, CAP, CSSLP, etc. the CSP could have some level of assurance that the assessor conducting the assessment has evidence of cloud security knowledge" [11].

"The criteria of an independent assessor(s) or assessment team within the Cloud should include a mix of skills and proficiencies … "

"… a key criteria that should be included as part of the selection criterion when identifying qualified and "capable" independent assessors or members of an assessment team is certifications that establish a baseline of cloud security knowledge" [12].

service meets FedRAMP security requirements through a conformity assessment[56] process. To ensure assessments of cloud services are conducted in a unified and standard approach, enabling a "do once, use many times" approach, organizations conducting the security assessments will need to be accredited to ensure they meet the minimum requirements of independence and competence.[57]

SUMMARY

In this chapter, FedRAMP was introduced through a detailed discussion of the program goals and objectives, and its role in supporting the secure adoption of cloud computing services. The program's governing documents (i.e., Policy Memo, CONOPS) provide insight into how the program operates. In addition, the primary stakeholders were also briefly discussed as it relates to their roles and responsibilities for the governance and execution of FedRAMP process areas. Through a review of the FedRAMP process areas defined within the FedRAMP CONOPS, a mapping to NIST RMF provides context into the similarities and differences between the FedRAMP implementation of those processes defined in NIST standards and guidance references.

[56] From Global Standards Information, Conformity Assessment [Internet]. Maryland: National Institute of Standards and Technology [cited 2012 Mar 17]. Available from: http://gsi.nist.gov/global/index.cfm/L1-5/L2-45. *"Conformity assessment procedures provide a means of ensuring that the products, services, systems, persons, or bodies have certain required characteristics, and that these characteristics are consistent from product to product, service to service, system to system, etc."*

[57] Breitenberg, M. NISTIR 6014, The ABC's of the US Conformity Assessment System. Maryland: National Institute of Standards and Technology; 1997. *"A prescribed set of rules, conditions, or requirements concerning definitions of terms; classification of components; specification of materials, performance, or operations; delineation of procedures; or measurement of quantity and quality in describing materials, products, systems, services, or practices."*

Finally, the FedRAMP 3PAO program was introduced highlighting the role of the 3PAO in ensuring CSPs are in conformance with the FedRAMP security and privacy requirements.

References

[1] Mel P. ISACA national capital area chapter, Session #4: federal risk and authorization management program (FedRAMP). Maryland: National Institute of Standards and Technology; 2010.

[2] Kundra V. Proposed security assessment & authorization for US government cloud computing, draft version 0.96. Washington, DC: CIO Council; 2010.

[3] VanRoekel S. Office of Management and Budget (OMB) memorandum, security authorization of information system in cloud computing environments. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011.

[4] FedRAMP Program Management Office (PMO). Federal risk and authorization management program (FedRAMP), agency day. Washington: US General Services Administration; 2012.

[5] E-Government Act of 2002 [Internet]. Washington: US Government Printing Office; [cited Dec 5, 2011]. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm.

[6] FedRAMP Program Management Office (PMO). FedRAMP concept of operations (CONOPS) version 1.1. Washington: US General Services Administration; 2012.

[7] Joint Task Force Transformation Initiative Interagency Working Group. NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010.

[8] Zients J, Kundra V, Schmidt H. Office of Management and Budget (OMB) memorandum 10–15, FY 2010 reporting instructions for the federal information system management act and agency privacy management. Washington, DC: Executive Office of the President, Office of Management and Budget; 2010.

[9] FedRAMP Program Management Office (PMO). FedRAMP continuous monitoring strategy and guide version 1.0. Washington: US General Services Administration; 2012.

[10] FedRAMP Program Management Office (PMO). General FedRAMP FAQ [Internet]. Washington: US General Services Administration [cited Mar 15, 2011]. <http://www.gsa.gov/portal/content/118887>.

[11] Metheny M. Selecting a 3PAO with assessors that have the certificate of cloud security knowledge (CCSK) [Internet]. Florida: International Information Systems Security Certification Consortium (ISC)2 Blog [cited April 1, 2012]. <http://blog.isc2.org/isc2_blog/2012/04/selecting-a-3pao-with-assessors-that-have-the-certificate-of-cloud-security-knowledge-ccsk.html>.

[12] Metheny, M. Selecting an Independent Third Party Assessor [Internet]. Washington, DC: FedRAMP.net [cited April 1, 2012]. <http://www.fedramp.net/selecting-an-independent-third-party-assessor>.

[13] FedRAMP Program Management Office (PMO). Guide to Understanding FedRAMP Version 1.0. Washington: US General Services Administration; 2012.

This page is intentionally left blank

CHAPTER

The FedRAMP Cloud Computing Security Requirements

9

INFORMATION IN THIS CHAPTER:

- Security Control Selection Process
- FedRAMP Cloud Computing Security Requirements

SECURITY CONTROL SELECTION PROCESS

The Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) selected security controls from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 low and moderate security control baselines and supplemented with additional security controls and enhancements to address the unique risks to cloud computing environments. These risks included multi-tenancy, visibility, control/responsibility, shared resource pooling, and trust [1]. The FedRAMP security control baselines were developed through a multi-step process focused on defining a standardized set of security requirements for the cost-effective authorization of cloud services for use by the federal government. As discussed in Chapter 5, the security control selection process involved the application of three steps:

- Selecting the initial security control baseline.
- Tailoring the security control baseline.
- Supplementing the security control baseline.

Since the FedRAMP program is meant to be a consistent, government-wide approach to security assessment and authorization, the final security control baselines creates a government-wide overlay[1] that identifies specific security requirements for "cloud-based information systems that are uniformly applied to all federal agencies procuring or implementing cloud services" [2].

[1] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"An overlay is a fully specified set of security controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance."*

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00009-5

Selecting the Security Control Baseline

The FedRAMP security control baselines operates at the low- or moderate-impact level, where low and moderate categorization is equally applied across all of the security objectives (*confidentiality*, *integrity*, and *availability*) for the cloud service.

For cloud services applying the FedRAMP low baseline, the security control baseline was developed based on the following security categorization:

> Security Category $_{\text{cloud service}}$ = {(**confidentiality**, *low*), (**integrity**, *low*), (**availability**, *low*)}

where the value for potential impact to the loss of confidentiality, integrity, and availability is low.

For cloud services applying the FedRAMP moderate baseline, the security control baseline was developed based on the following security categorization:

> Security Category $_{\text{cloud service}}$ = {(**confidentiality**, *moderate*), (**integrity**, *moderate*), (**availability**, *moderate*)}

where the value for potential impact to the loss of confidentiality, integrity, and availability is moderate.

Tailoring and Supplementing Security Control Baseline

The FedRAMP security control baselines[2] were developed through the application of the NIST Risk Management Framework (RMF)[3] tailoring process. As discussed previously, the tailoring process is the second step of the security control selection process and includes the assignment of specific values to the organization-defined security control parameters.[4] Some security controls included within NIST SP 800-53, Appendix F—Security Control Catalog, have embedded parameters[5] that are

[2] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4, (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"Baseline controls are the starting point for the security control selection process."*

[3] Chapter 5 discussed the risk management activities involved in the application of the Risk Management Framework (RMF).

[4] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4, (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"Organizations may choose to define specific values for security control parameters in policies, procedures, or guidance (which may be applicable to more than one information system) referencing the source documents in the security plan in lieu of explicitly completing the assignment/selection statements within the control as part of the plan."*

[5] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"Values for organization-defined parameters are adhered to unless more restrictive values are prescribed by applicable federal laws, Executive Orders, directives, policies, standards, guidelines, or regulations."*

designed to provide flexibility when defining the specification for the security control and enhancement(s) necessary to support the definition of government-wide security requirements for the secure use of cloud computing services.

After the initial security control baseline was tailored, the FedRAMP JAB supplemented the baseline with additional security controls and enhancements identified as necessary to sufficiently protect federal information within a cloud computing environment. In addition to the requirements defined in the FedRAMP security controls, the FedRAMP JAB defined additional requirements through security control addendum [2].

FedRAMP Cloud Computing Overlay

The FedRAMP cloud computing overlay[6] is a government-wide set of security controls that are based on a focused look at the security capabilities and requirements needed to protect federal information within low- and moderate-impact cloud services. The application of an overlay does not limit Cloud Service Providers (CSPs) or federal agencies from tailoring or supplementing the FedRAMP security control baselines, rather it creates a " community-wide or specialized set of security controls for information system and organizations" [2] based on a consensus[7] of those within the community that the requirements should be broadly applied to multiple information systems (and cloud services) that meet a specific target characteristic (i.e., the FedRAMP control baselines can be further refined based on a specific service or deployment model).

FEDRAMP CLOUD COMPUTING SECURITY REQUIREMENTS

The FedRAMP "Policy Memo," as discussed in Chapter 8, is the overarching policy that covers all commercial and non-commercial cloud services, including all cloud deployment and service models with the exception[8] of a private cloud operating

[6] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4, (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"An overlay is a fully specified set of security controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance."*

[7] From Joint Task Force Transformation Initiative. Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"The overlay concept is most effective when communities of interest work together to create consensus-based overlays that are not duplicative."*

[8] From FedRAMP Program Management Office (PMO). General FedRAMP FAQ [Internet]. Washington: US General Services Administration [cited 2011 Mar 13]. Available from: http://www.gsa.gov/portal/content/118875. *"Private cloud deployments intended for single organizations and implemented fully within Federal facilities are the only exception."*

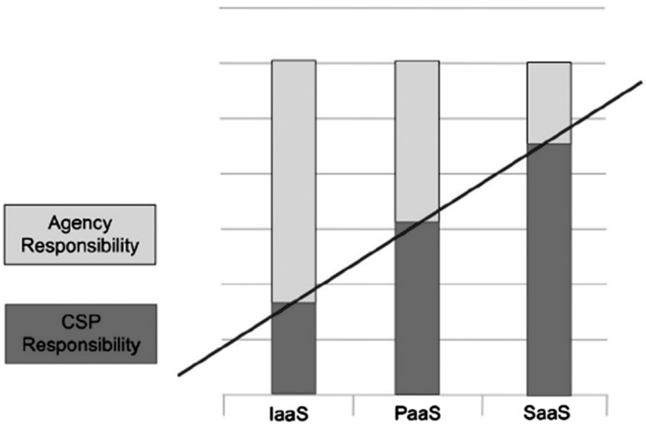


FIGURE 9.1 Security Control Responsibilities [3]

on-premise, and which provides services to only the owning organization (i.e., no external users, including other organizational entities within the same federal agency). Since CSPs can operate as either a public (i.e., federal or state government) or private sector organization or both, potentially complex cloud relationships can be created where security control assignment and ownership can be difficult to determine. Therefore, all stakeholders should participate in planning and coordinating the development of cloud-specific contracts (or other end-user agreements).[9]

The scope of the contracts (or agreements) should provide a clear definition of the governance over the cloud service environment (i.e., the policies, procedures, standards, guidelines, and roles and responsibilities that would be applied). In addition, the contracts (or agreements) should provide a clear delineation of the security control responsibility,[10] similar to Figure 9.1, including any applicable policies and procedures that would satisfy the requirements for the security controls. As an example, the FedRAMP CONOPS requires CSPs to submit information security policies

[9] From Federal CIO Council, Chief Acquisition Officer Council. Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service. Washington: Federal CIO Council; 2012. *"Any contract provisions regarding controlling law, jurisdiction, and indemnification arising out of a Federal agency's use of a CSP environment must align with Federal statutes, policies, and regulations; and compliance should be defined before a contract award. This may be done through a separate document or be included in the actual contract."*

[10] From FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. *"The FedRAMP Control Implementation Summary (CIS) summarizes the control ownership and indicates which controls are owned and managed by the CSP and which controls are owned and managed by the leveraging agency."*

governing their cloud service, as described in the System Security Plan (SSP),[11] to the FedRAMP PMO as part of the FedRAMP security authorization process.

The delineation should include any applicable policies and procedures that would apply to the implementation of the FedRAMP security controls. Since CSPs are required to submit information security policies and procedures governing their cloud service as described in the FedRAMP SSP[12] Template to the FedRAMP PMO as part of the FedRAMP security authorization process, CSPs should at minimum have established security policies that govern all of the FedRAMP security requirements that are applicable to their cloud service layer.

The assignment of responsibility for security controls is an essential activity that requires identifying situations where there is potential shared responsibilities (or hybrid controls). For example, a CSP may implement the Incident Response Policy and Procedures security control (IR-1) as a hybrid control with the policy portion of the control deemed to be common and applied as a corporate responsibility, and the procedures portion of the control deemed to be system-specific [4]. The FedRAMP PMO established the Control Implementation Summary (CIS) document to be completed by the CSP to aid in communicating the ownership and responsibility of the security controls between the CSP and the federal agency customer.

Policy and Procedures

The Federal Information Security Management Act (FISMA)[13] requires the highest-level senior executive within an organization (e.g., head of the federal agency, chief executive officer) with the overall responsibility to provide for the information security protections and to ensure the development, implementation, and maintenance of information security policies, procedures, and control techniques. The policies, procedures, and control techniques must address all applicable requirements, including those issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST), except where authority is delegated to other organizations (e.g., the Secretary of Defense for US Department of Defense (DoD) information systems).

In each of the security control families (e.g., security assessment and authorization, configuration management, access control), the first control, identified as the

[11] From FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. *"The SSP details the security authorization boundary, how the implementations address each required control and enhancement in the selected control baseline, descriptions of roles and responsibilities, and expected behavior of individuals with system access."*

[12] From FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. *"The SSP details the security authorization boundary, how the implementations address each required control and enhancement in the selected control baseline, descriptions of roles and responsibilities, and expected behavior of individuals with system access."*

[13] FISMA was discussed in detail in Chapter 5, Applying the Risk Management Framework.

"XX-1" security controls, requires the development of security policies[14] that address the requirements that must be implemented within the information system or by the organization.[15] CSP security policies should include at minimum the purpose[16] of the policy, the scope,[17] the roles and responsibilities,[18] and compliance.[19] The FedRAMP "Policy Memo"[20] issued by the OMB defines the government-wide security program,[21] and the security and authorization policy for addressing the security and authorization of cloud computing environments. Through the implementation of an information security program plan,[22] the organization can effectively centralize those security controls deemed independent of a particular cloud service and instead manage them as part of the overarching information security program.

[14] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance."*

[15] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. *"The federal agency or subordinate organization that owns the authorization package. The information system may not be owned by the same organization that owns the authorization package, for example, in situations where the system/services are provided by an external provider."*

[16] From Burrows, J., McNulty, F., Katzke, S., Gilbert, I., Steinauer, D. NIST Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook. Maryland: National Institute of Standards and Technology; 1995. *"Program policy normally includes a statement describing why the program is being established. This may include defining the goals of the program."*

[17] From Burrows, J., McNulty, F., Katzke, S., Gilbert, I., Steinauer, D. NIST Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook. Maryland: National Institute of Standards and Technology; 1995 *"Program policy should be clear as to which resources—including facilities, hardware, and software, information, and personnel—the computer security program covers."*

[18] From Burrows, J., McNulty, F., Katzke, S., Gilbert, I., Steinauer, D. NIST Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook. Maryland: National Institute of Standards and Technology; 1995. *"Once the computer security program is established, its management is normally assigned to either a newly-created or existing office."*

[19] From Burrows, J., McNulty, F., Katzke, S., Gilbert, I., Steinauer, D. NIST Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook. Maryland: National Institute of Standards and Technology; 1995. *"Addresses two issues, general compliance, to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components and the use of specified penalties and disciplinary actions."*

[20] The FedRAMP "Policy Memo" includes all of the key components of a policy such as purpose, scope, roles and responsibility, and compliance.

[21] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"Security program policies and procedures at the organization level may make the need for system-specific policies and procedures"*.

[22] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization."*

TIP

Standards, Guidelines, and Procedures

To assist CSPs and federal agencies in implementing policies, standards, guidelines, and procedures should be used. Standards and guidelines, such as those developed by NIST under a statutory responsibility, establish minimum requirements promulgated from legislative mandates "to support the implementation of and compliance with the Federal Information Security Management Act" [5]. Whereas other standards and guidelines such as the NIST SPs, Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs),[23] or National Security Agency Information Assurance (IA) Mitigation Guidelines[24] focus on providing specific methods or techniques for ensuring the security of a solution. Standards and guidelines can focus on a general concept such as sever security,[25] secure communication[26] or secure operations,[27] while others may target a specific technology (i.e., virtualization[28] or IPv6[29] or security feature (i.e., encryption[30] or security automation[31]). Procedures are more scoped to the operating environment (i.e., operational personnel, facility, and system operations) and provide the detailed steps that address how the policies, standards, and guidelines are applied within an operational context such as credential management or performing audit log management.

Harmonizing FedRAMP Requirements

The FedRAMP "Policy Memo" established a standard set of security requirements that would be used for the authorization and ongoing continuous monitoring of cloud services.[32] In addition, the FedRAMP security requirements could be supplemented with additional federal agency-specific security and privacy requirements, or even

[23] *Security Technical Implementation Guides (STIGs) Security Checklists*. Available from: http://iase.disa.mil/stigs/.

[24] *IA Mitigation Guidance*. Available from: http://www.nsa.gov/ia/mitigation_guidance/index.shtml.

[25] NIST Special Publication (SP) 800-123, *Guide to General Server Security*. Available from: http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf. NIST SP 800-113, *Guide to SSL VPNs*. Available from: http://csrc

[26] NIST Special Publication (SP) 800-113, *Guide to SSL VPNs*. Available from: http://csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf.

[27] NIST Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems*. Available from: http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf.

[28] NIST Special Publication (SP) 800-125, *Guide to Security for Full Virtualization Technologies*. Available from: http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf.

[29] NIST Special Publication (SP) 800-119, *Guidelines for the Secure Deployment of IPv6*. Available from: http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf.

[30] NIST Special Publication (SP) 800-130, *A Framework for Designing Cryptographic Key Management Systems*. Available from: http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-130.

[31] NIST Special Publication (SP) 800-126, *The Technical Specific for the Security Content Automation Protocol (SCAP)*. Available from: http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf.

[32] At the time of the FedRAMP memo publication, only NIST-defined low-and moderate-impact information systems were considered within the scope of FedRAMP.

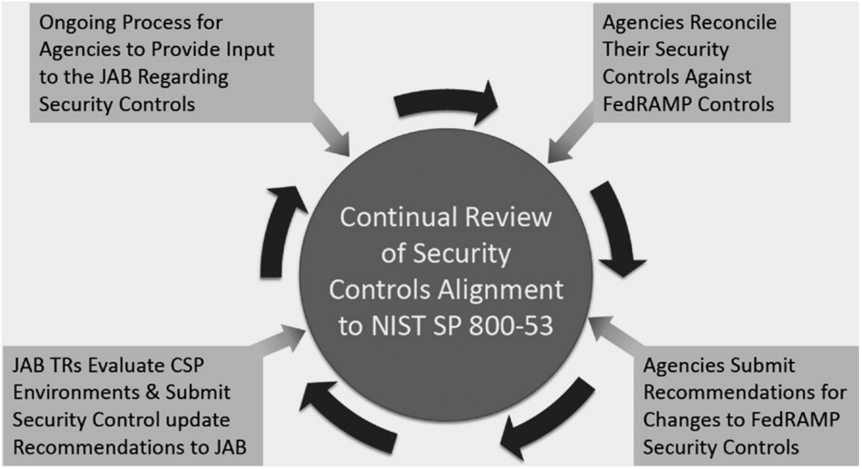

Ongoing Process for Agencies to Provide Input to the JAB Regarding Security Controls
Agencies Reconcile Their Security Controls Against FedRAMP Controls
Continual Review of Security Controls Alignment to NIST SP 800-53
JAB TRs Evaluate CSP Environments & Submit Security Control update Recommendations to JAB
Agencies Submit Recommendations for Changes to FedRAMP Security Controls

FIGURE 9.2 Maintenance of Security Controls [6]

incur changes through updates to NIST SP 800-53 and by the JAB[33] review process. Therefore, a harmonization governance process,[34] similar to Figure 9.2, may be used by the FedRAMP PMO to maintain and elicit changes to the FedRAMP security controls, to include changes in security control requirements.

Through a continual review process,[35] input from multiple sources can be used by the JAB to harmonize the FedRAMP security controls as part of a review and adjudication. Example input could include feedback from federal agencies on the adequacy of the FedRAMP security control requirements, an evaluation by JAB Technical Representatives (TRs) of CSP environments, or the reconciliation with federal agency–specific security and privacy requirements. In addition, all federal

[33] From VanRoekel, S. Office of Management and Budget (OMB) Memorandum, Security Authorization of Information System in Cloud Computing Environments. Washington: Executive Office of the President, Office of Management and Budget; 2011. *The JAB shall "define and regularly review the FedRAMP security authorization requirements in accordance with the Federal Information Security Management Act of 2002 (FISMA) and DHS guidance."*

[34] From VanRoekel, S. Office of Management and Budget (OMB) Memorandum, Security Authorization of Information System in Cloud Computing Environments. Washington: Executive Office of the President, Office of Management and Budget; 2011. *The FedRAMP PMI will create "a methodology for harmonizing agency-specific security and privacy controls with the FedRAMP security authorization requirements."*

[35] From Coleman, C., Spires, R., Takai, T. Federal Risk and Authorization Management Program Joint Authorization Board Charter Version 1.0. Washington: FedRAMP Program Management Office, US General Services Administration; 2012. *"The JAB will work with the FedRAMP PMO to establish methods for regular input by Executive departments and agencies to ensure the FedRAMP security authorization requirements are meeting the needs of the Federal government."*

agencies (and contractors)[36] are required to be in compliance with NIST publications[37] one year[38] from date of publication. Therefore, changes to the NIST SP 800-53 could also require changes and updates to the FedRAMP security controls.

Assurance of External Service Providers Compliance

FISMA requires agencies to provide security protections "... commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or other organization on behalf of an agency" [7]. In addition, OMB requires federal agencies to ensure appropriate information security oversight capabilities exist for contractors and other users with privileged access to federal data and systems.

CSPs, regardless of the deployment and service model, are required to meet the same requirements when processing, storing, or transmitting federal information or are operating on behalf of the federal government. The integration of FedRAMP security requirements into the terms and conditions of contracts and service level agreements (SLAs)[39] provides mechanisms when defining roles and responsibilities. The FedRAMP PMO provides standard contract clauses,[40] control-specific contract clauses,[41] and accompanying SLA guidance[42] covering all FedRAMP

[36] From FedRAMP Program Management Office (PMO). FedRAMP Standard Contract Language, Washington: US General Services Administration; 2012. *"Contractor shall refer to cloud service providers, or contract holders who are providing cloud computing services to the Federal Government through this contract."*

[37] From Lew, J. Office of Management and Budget (OMB) Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. Washington: Executive Office of the President, Office of Management and Budget; 2011. *"For information systems under development or for legacy systems undergoing significant changes, agencies are expected to be in compliance with the NIST publications immediately upon deployment of the information system."*

[38] From Lew, J. Office of Management and Budget (OMB) Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. Washington: Executive Office of the President, Office of Management and Budget; 2011. *"The one year compliance date for revisions to NIST publications applies to new and/or updated material in the publications."*

[39] Example sources for defining service levels can include the Open Data Center Alliance (ODCA) Usage Models available from: http://www.opendatacenteralliance.org/ourwork/usagemodels.

[40] FedRAMP Standard Contract Clauses. Available from: http://www.gsa.gov/graphics/staffoffices/FedRAMP_Standard_Contractual_Clauses_062712.pdf.

[41] FedRAMP Control-Specific Contract Clauses. Available from: http://www.gsa.gov/graphics/staffoffices/FedRAMP_Control_Specific_Clauses_062712.pdf.

[42] In February 2012, the Federal CIO Council and the Chief Acquisition Officers Council published a best practices guide for *Creating Effective Cloud Computing Contracts for the Federal Government* to provide federal agencies with best practices for acquiring IT as a service.

NOTE

The Federal Acquisition Regulation (FAR) covers the acquisition of IT supplies and services used by federal agencies. The requirements within the FAR include applicable provisions with references to address information security and privacy as part of the acquisition process. These requirements include

- FAR 7.103(u)—"Ensuring that agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 US C. 3544), OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from the Department of Commerce's National Institute of Standards and Technology" [8].
- FAR 11.102—"Agencies shall select existing requirements documents or develop new requirements documents that meet the needs of the agency in accordance with the guidance contained in the Federal Standardization Manual, FSPM-0001; for DoD components, DoD 4120.24-M, Defense Standardization Program Policies and Procedures; and for IT standards and guidance, the Federal Information Processing Standards Publications (FIPS PUBS)" [9].
- FAR 39.101(d)—"In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated" [10].
- FAR 52.239-1(a) "Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government." [13].
- FAR 52.239-1(b) "To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases."
- FAR 52.239-1(c) "If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party."

requirements [3]. Although CSPs are responsible for ensuring compliance with the FedRAMP security requirements the overall responsibility for mitigating risks in using cloud services is retained with the federal agency customer.

Approaches to Implementing FedRAMP Security Controls

Decisions made as part of the security control selection process are driven by the organization's determination of the adequate protection for a given information system within a target operating environment. The decisions made during the risk management activities aid in establishing the risk-based information such as assumptions, constraints, and rationale needed for addressing security within the information system. This information supports the implementation of security controls based on a risk-based approach that requires an understanding of the potential impacts to the organization's mission or business processes and those organizations that rely upon the information system. The potential impact is based on the compromise of one or more security objectives[43] (i.e., loss of confidentiality, integrity, or availability).

Some information systems are in the development process (i.e., *new development*), while others may already be in production (i.e., *legacy*). Depending on the state of the information system, security controls may be part of the initial requirements definition or applied as part of the change management function. If the information system is in the development process, the integration of security controls can be applied as part of the normal system development lifecycle (SDLC).[44] However, if the information system is already in production, a gap analysis approach can be used to assist the organization in fully understanding what is in place and what additional security controls will need to be applied to address the differences in the requirements gap. In some circumstances, compensating security controls may even need to be identified and applied where existing security controls that are already in place have been determined to be insufficient to effectively mitigate potential risks.

CSPs can apply similar techniques when implementing the FedRAMP security controls. Since cloud services may present different risks than traditional IT environments, the CSP should conduct an additional analysis to identify where the gaps exist (i.e., within the different cloud service models and technology implementations) and who has the overall responsibility (CSP or federal agency) for addressing the weaknesses or deficiencies. As an example, Figure 9.3 illustrates a high-level gap analysis exercise that CSPs could use to identify the gaps in their security capabilities and features based on what is built in.

[43] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"Security controls are typically deployed as a unified set to achieve a desired security capability. The loss of one security objective (e.g. integrity) can adversely affect the other objectives (e.g. confidentiality and availability). When selecting security controls for nondisclosure purposes, organizations consider the security categorization of user data and system-level data—where system data may require stronger protection in the form of additional security controls."*

[44] NIST Special Publication (SP) 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*. Available from: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf.

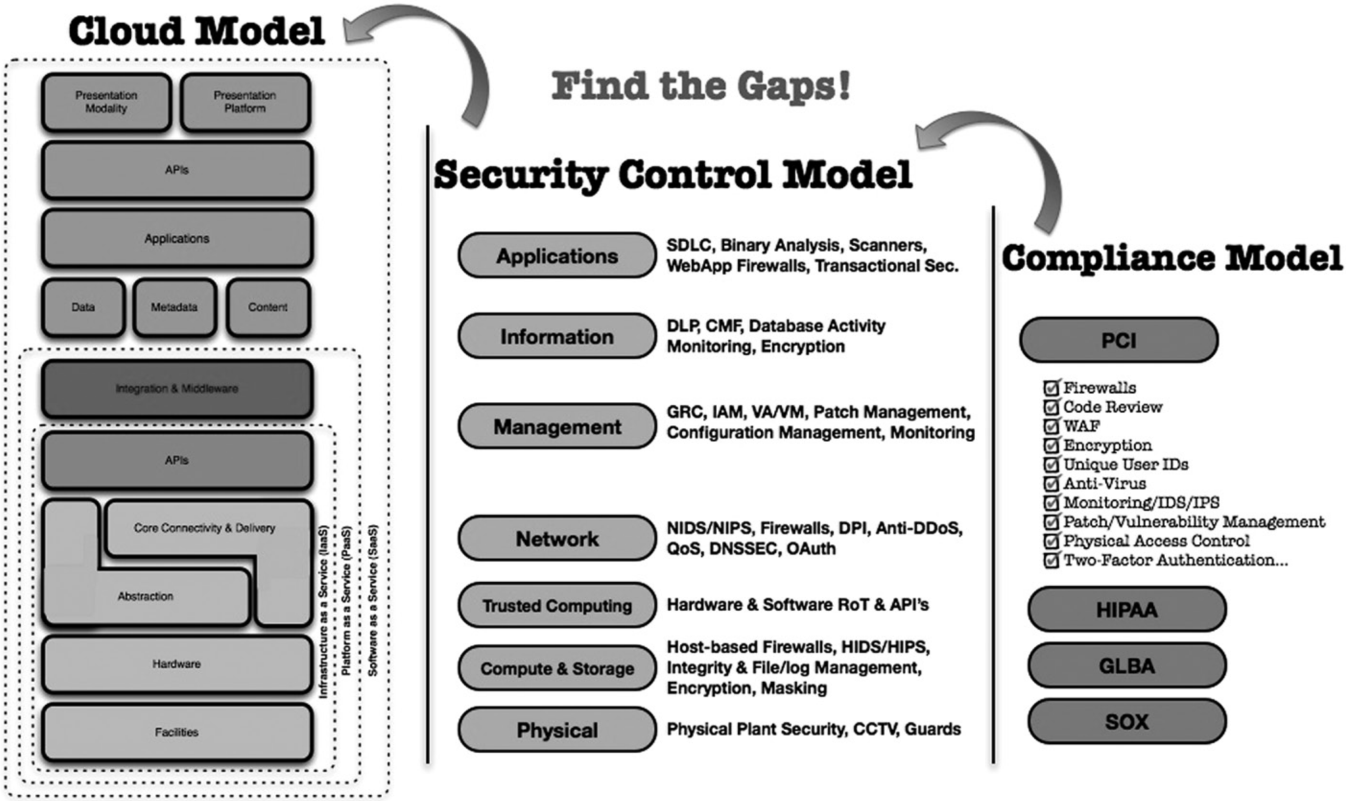

Cloud Model
Presentation Modality
Presentation Platform
APIs
Applications
Data
Metadata
Content
Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Find the Gaps!
Security Control Model
Applications
SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information
DLP, CMF, Database Activity Monitoring, Encryption
Management
GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network
NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing
Hardware & Software RoT & API's
Compute & Storage
Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical
Physical Plant Security, CCTV, Guards
Compliance Model
PCI
☑ Firewalls
☑ Code Review
☑ WAF
☑ Encryption
☑ Unique User IDs
☑ Anti-Virus
☑ Monitoring/IDS/IPS
☑ Patch/Vulnerability Management
☑ Physical Access Control
☑ Two-Factor Authentication...
HIPAA
GLBA
SOX

FIGURE 9.3 Cloud Security Reference Model [11]

TIP

Some CSPs have already aligned with other regulatory or industry control frameworks such as ISO/IEC/27001 27002, ISACA COBIT, PCI DSS, and NIST 800-53. Therefore, the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)[45] provides an industry consensus framework that has been developed as a tool[46] for use by CSPs to integrate FedRAMP into their existing integrated security framework and to assist CSPs in conducting a crosswalk to determine the differences in their existing security and compliance program with the FedRAMP security requirements.

The gap analysis exercise include the following three steps [11]:

1. Classifying the service against the cloud model (e.g., IaaS, PaaS, or SaaS).
2. Map the existing security architecture against the cloud model.
3. Map the FedRAMP security requirements (identified as the compliance model) against the security architecture and the cloud model.

Using the steps in the gap analysis exercise, CSPs can use the preliminary information to complete the first 3 steps of the NIST RMF,[47] including determining the potential gaps in achieving the target FedRAMP security control baselines (low- or moderate-impact) based on their own application of the information security categorization process when completing the Federal Information Processing Standards (FIPS) 199 worksheet. In addition, this information can help them begin the process of documenting the Control Tailoring Workbook (CTW) and CIS, both discussed in Chapter 8.

FedRAMP Security Control Requirements

The FedRAMP security control requirements provide the minimum security control baseline requirements for cloud computing environments. These security controls were based on the minimum assurance requirements included in the NIST SP 800-53 [4] and the FedRAMP Security Controls [12].

[45] *Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)*. Available from: https://cloudsecurityalliance.org/research/ccm/.

[46] NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Appendix H provides a security control mapping between NIST Special Publication (SP) 800-53 controls and ISO/IEC 27001 (Annex A) controls.

[47] Chapter 5 discussed the risk management activities involved in the application of the Risk Management Framework (RMF).

AC-1	**Access Control Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*
AC-2	**Account Management**
Control Requirement:	The organization manages information system accounts, including: **a.** Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); **b.** Establishing conditions for group membership; **c.** Identifying authorized users of the information system and specifying access privileges; **d.** Requiring appropriate approvals for requests to establish accounts; **e.** Establishing, activating, modifying, disabling, and removing accounts; **f.** Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; **g.** Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; **h.** Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users. **i.** Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and **j.** Reviewing accounts *at least annually*.

AC-2	**Account Management**
Control Enhancements:	**1.** The organization employs automated mechanisms to support the management of information system accounts. **2**. The information system automatically terminates temporary and emergency accounts after *no more than ninety days for temporary and emergency account types*. **3.** The information system automatically disables inactive accounts after *ninety days for user accounts and after a JAB approved and accepted service provider defined time period for non-user accounts (e.g., accounts associated with devices)*. **4.** The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals. **7.** The organization: **a.** Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and **b.** Tracks and monitors privileged role assignments.
References:	
AC-3	**Access Enforcement**
Control Requirement:	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.
Control Enhancements:	**3.** The information system enforces role-based access control over all users and resources where the policy rule set for each policy specifies: **a.** Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and **b.** Required relationships among the access control information to permit access. The service provider: **a.** Assigns user accounts and authenticators in accordance with service provider's role-based access control policies; **b.** Configures the information system to request user ID and authenticator prior to system access; and

AC-3	**Access Enforcement**
	c. Configures the databases containing federal information in accordance with service provider's security administration guide to provide role-based access controls enforcing assigned privileges and permissions at the file, table, row, column, or cell level, as appropriate.
References:	
AC-4	**Information Flow Enforcement**
Control Requirement:	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.
References:	
AC-5	**Separation of Duties**
Control Requirement:	The organization: **a.** Separates duties of individuals as necessary, to prevent malevolent activity without collusion; **b.** Documents separation of duties; and **c.** Implements separation of duties through assigned information system access authorizations.
References	
AC-6	**Least Privilege**
Control Requirement:	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
Control Enhancements:	**1.** The organization explicitly authorizes access to a *JAB approved and accepted service provider defined list of security functions*. **2.** The organization requires that users of information system accounts, or roles, with access to *all security functions*, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.
References:	

AC-7	**Unsuccessful Login Attempts**
Control Requirement:	The information system: **a.** Enforces a limit of *no more than three* consecutive invalid login attempts by a user during a *fifteen minute time period*; and **b.** Automatically *locks the account/node for thirty minutes* when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.
References:	
AC-8	**System Use Notification**
Control Requirement:	The information system: **a.** Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a US Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording;**b.** Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and **c.** For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system. The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB. The service provider shall determine how System Use Notification is going to be verified and provide appropriate

	periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB. Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided. If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB.
References:	
AC-10	**Concurrent Session Control**
Control Requirement:	The information system limits the number of concurrent sessions for each system account to *one session*.
References:	
AC-11	**Session Lock**
Control Requirement:	The information system: **a.** Prevents further access to the system by initiating a session lock after *fifteen minutes* of inactivity or upon receiving a request from a user; and **b.** Retains the session lock until the user reestablishes access using established identification and authentication procedures.
Control Enhancements:	**1.** The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.
References:	• OMB Memorandum 06-16, *Protection of Sensitive Agency Information*.
AC-14	**Permitted Actions without Identification and Authentication**
Control Requirement:	The organization: **a.** Identifies specific user actions that can be performed on the information system without identification or authentication; and **b.** Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

AC-14	**Permitted Actions without Identification and Authentication**
Control Enhancements:	**1.** The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.
References:	

AC-16	**Security Attributes**
Control Requirement:	The information system supports and maintains the binding of *JAB approved and accepted service provider defined security attributes (if capability is offered)* to information in storage, in process, and in transmission.
References:	

AC-17	**Remote Access**
Control Requirement:	The organization: **a.** Documents allowed methods of remote access to the information system; **b.** Establishes usage restrictions and implementation guidance for each allowed remote access method; **c.** Monitors for unauthorized remote access to the information system; **d.** Authorizes remote access to the information system prior to connection; and **e.** Enforces requirements for remote connections to the information system.
Control Enhancements:	**1.** The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. **2.** The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. **3.** The information system routes all remote accesses through a limited number of managed access control points. **4.** The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. **5.** The organization monitors for unauthorized remote connections to the information system *continuously, real-time*, and takes appropriate action if an unauthorized connection is discovered.

AC-17	**Remote Access**
	7. The organization ensures that remote sessions for accessing *a JAB approved and accepted service provider defined list of security functions and security-relevant information* employ (Assignment: *organization-defined additional security measures*) and are audited. **8.** The organization disables tftp (trivial ftp), X-Windows, Sun Open Windows; FTP; TELNET; IPX/SPX; NETBIOS; Bluetooth; RPC-services, like NIS or NFS; rlogin, rsh, rexec; SMTP (Simple Mail Transfer Protocol); RIP (Routing Information Protocol); DNS (Domain Name Services); UUCP (Unix-Unix Copy Protocol); NNTP (*Network News Transfer Protocol*); NTP (*Network Time Protocol*); Peer-to-Peer except for explicitly identified components in support of specific operational requirements where networking protocols implemented by the service provider are approved and accepted by the JAB.
References:	• NIST SP 800-46*, Guide to Enterprise Telework and Remote Access Security.* • NIST SP 800-77, *Guide to IPsec VPNs.* • NIST SP 800-113, *Guide to SSL VPNs.* • NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access.* • NIST SP 800-121, *Guide to Bluetooth Security.*
AC-18	**Wireless Access**
Control Requirement:	The organization: **a.** Establishes usage restrictions and implementation guidance for wireless access; **b.** Monitors for unauthorized wireless access to the information system; **c.** Authorizes wireless access to the information system prior to connection; and **d.** Enforces requirements for wireless connections to the information system.
Control Enhancements:	**1.** The information system protects wireless access to the system using authentication and encryption. **2.** The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points *at least quarterly*, and takes appropriate action if an unauthorized connection is discovered.

AC-18	**Wireless Access**
References:	• NIST SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks.* • NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS).* • NIST SP 800-97, *Guide to Intrusion Detection and Prevention Systems (IDPS).*
AC-19	**Access Control for Mobile Devices**
Control Requirement:	The organization: **a.** Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; **b.** Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems **c.** Monitors for unauthorized connections of mobile devices to organizational information systems; **d.** Enforces requirements for the connection of mobile devices to organizational information systems; **e.** Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; **f.** Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and **g.** Applies *JAB approved and accepted service provider defined inspection and preventive measures* to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
Control Enhancements:	**1.** The organization restricts the use of writable, removable media in organizational information systems. **2.** The organization prohibits the use of personally owned, removable media in organizational information systems. **3.** The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

AC-19	**Access Control for Mobile Devices**
References:	• NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*. • NIST SP 800-124, *Guidelines on Cell Phone and PDA Security.*
AC-20	**Use of External Information Systems**
Control Requirement:	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: **a.** Access the information system from the external information systems; and **b.** Process, store, and/or transmit organization-controlled information using the external information systems.
Control Enhancements:	**1.** The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: **a.** Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or **b.** Has approved information system connection or processing agreements with the organizational entity hosting the external information system. **2.** The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.*
AC-22	**Publicly Accessible Content**
Control Requirement:	The organization: **a.** Designates individuals authorized to post information onto an organizational information system that is publicly accessible; **b.** Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; **c.** Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;

AC-22	**Publicly Accessible Content**
	d. Reviews the content on the publicly accessible organizational information system for nonpublic information *at least quarterly*; and **e.** Removes nonpublic information from the publicly accessible organizational information system, if discovered.
References:	

Awareness and Training (AT)

AT-1	**Security Awareness and Training Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
References	• NIST SP 800-12, *An Introduction to Computer Security.* • NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* • NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*
AT-2	**Security Awareness**
Control Requirement:	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and *at least annually* thereafter.
References:	• C.F.R. Part 5 Subpart C (5 C.F.R. 930.301), *Information Systems Security Awareness Training Program.* • NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program.*
AT-3	**Security Training**
Control Requirement:	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) *at least every three years* thereafter.

AT-3	**Security Training**
References:	• C.F.R. Part 5 Subpart C (5 C.F.R. 930.301), *Information Systems Security Awareness Training Program.* • NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* • NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program.*
AT-4	**Security Training Records**
Control Requirement:	The organization: **a.** Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and **b.** Retains individual training records for *at least three years*.
References:	

Audit and Accountability (AU)

AU-1	**Audit and Accountability Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*
AU-2	**Auditable Events**
Control Requirement:	The organization: **a.** Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: *Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes*;

AU-2	**Auditable Events**
	b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; **c.** Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and **d.** Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited continually within the information system: *a JAB approved and accepted service provider defined subset of event from AU-2a to be audited*.
Control Enhancements:	**3.** The organization reviews and updates the list of auditable events *annually or whenever there is a change in the threat environment*. **4.** The organization includes execution of privileged functions in the list of events to be audited by the information system. *The service provider configures the auditing features of operating systems, databases, and applications to record security-related events, to include logon/logoff and all failed access attempts.*
References:	• NIST SP 800-92, *Guide to Computer Security Log Management.*
AU-3	**Content of Audit Records**
Control Requirement:	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.
Control Enhancements:	**1.** The information system includes *session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon in the JAB approved and accepted service provider defined types of audit records for audit events identified by type, location, or subject.*
References:	
AU-4	**Audit Storage Capacity**
Control Requirement:	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.
References:	

AU-5	**Response to Audit Processing Failures**
Control Requirement:	The information system: **a.** Alerts designated organizational officials in the event of an audit processing failure; and **b.** Takes the following additional actions: *low-impact: overwrite oldest audit records; moderate-impact: shut down.*
References:	
AU-6	**Audit Review, Analysis, and Reporting**
Control Requirement:	The organization: **a.** Reviews and analyzes information system audit records *at least weekly* for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and **b.** Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.
Control Enhancements:	**1.** The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. **3.** The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.
References:	
AU-7	**Audit Review, Analysis, and Reporting**
Control Requirement:	The information system provides an audit reduction and report generation capability.
Control Enhancements:	**1.** The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.
References:	
AU-8	**Time Stamps**
Control Requirement:	The information system uses internal system clocks to generate time stamps for audit records.

AU-8	**Time Stamps**
Control Enhancements:	**1.** The information system synchronizes internal information system clocks *at least hourly* with *http://tf.nist.gov/tf-cgi/servers.cgi*. *The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server. The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.*
References:	
AU-9	**Protection of Audit Information**
Control Requirement:	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
Control Enhancements:	**2.** The information system backs up audit records *at least weekly* onto a different system or media than the system being audited.
References:	
AU-10	**Non-Repudiation**
Control Requirement:	The information system protects against an individual falsely denying having performed a particular action.
Control Enhancements:	**5.** The organization employs FIPS-validated cryptography (e.g., DoD PKI class 3 or 4 token) to implement digital signatures. The service provider implements FIPS-140-2 validated cryptography (e.g., DOD PKI Class 3 or 4 tokens) for service offerings that include Software-as-a-Service (SaaS) with email.
References:	
AU-11	**Audit Record Retention**
Control Requirement:	The organization retains audit records for *at least ninety days* to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. *The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements.*
References:	

AU-12	**Audit Generation**
Control Requirement:	The information system: **a.** Provides audit record generation capability for the list of auditable events defined in AU-2 in *all information system components where audit capacity is deployed*; **b.** Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and **c.** Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.
References:	

Security Assessment and Authorization (CA)

CA-1	**Security Assessment and Authorization Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-37, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans* • NIST 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*
CA-2	**Security Assessments**
Control Requirement:	The organization: **a.** Develops a security assessment plan that describes the scope of the assessment including: – Security controls and control enhancements under assessment; – Assessment procedures to be used to determine security control effectiveness; and – Assessment environment, assessment team, and assessment roles and responsibilities.

CA-2	**Security Assessments**
	b. Assesses the security controls in the information system *at least annually* to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; **c.** Produces a security assessment report that documents the results of the assessment; and **d.** Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official-designated representative.
Control Enhancements:	**1.** The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-37,*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* • NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View.* • NIST 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations; Building Effective Security Assessment Plans* • NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment.*
CA-3	**Information System Connections**
Control Requirement:	The organization: **a.** Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; **b.** Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and **c.** Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems.*

CA-5	**Plan of Action and Milestones**
Control Requirement:	The organization: **a.** Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and **b.** Updates existing plan of action and milestones *at least quarterly* based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
References:	• OMB Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones.* • NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*
CA-6	**Security Authorization**
Control Requirement:	The organization: **a.** Assigns a senior-level executive or manager to the role of authorizing official for the information system; **b.** Ensures that the authorizing official authorizes the information system for processing before commencing operations; and **c.** Updates the security authorization *at least every three years or when a significant change occurs*.
References:	• OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources.* • OMB Memorandum *12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* • NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. • NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.
CA-7	**Continuous Monitoring**
Control Requirement:	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: **a.** A configuration management process for the information system and its constituent components; **b.** A determination of the security impact of changes to the information system and environment of operation;

CA-7	**Continuous Monitoring**
	c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and **d.** Reporting the security state of the information system to appropriate organizational officials *monthly*.
Control Enhancements:	**2.** The organization plans, schedules, and conducts assessments annually, unannounced, penetration testing, and in-depth monitoring to ensure compliance with all vulnerability mitigation procedures.
References:	• OMB Memorandum *12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. • NIST SP 800-37, *Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. • NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*. • NIST 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations; Building Effective Security Assessment Plans.* • NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*. • Website: www.us-cert.gov/cas/techalerts, *US-CERT Technical Cyber Security Alerts*.

Configuration Management (CM)

CM-1	**Configuration Management Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*. • NIST SP 800-100, *Information Security Handbook: A Guide for Managers*.

CM-2	**Baseline Configuration**
Control Requirement:	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.
Control Enhancements:	**1.** The organization reviews and updates the baseline configuration of the information system: **a.** *annually;* **b.** When required due to a *significant change;* and **c.** As an integral part of information system component installations and upgrades. **3.** The organization retains older versions of baseline configurations as deemed necessary to support rollback. **5.** The organization: **a.** Develops and maintains *a JAB approved and accepted service provider defined list of software programs authorized to execute on the information system;* and **b.** Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.
References:	• NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems.*
CM-3	**Configuration Change Control**
Control Requirement:	The organization: **a.** Determines the types of changes to the information system that are configuration controlled; **b.** Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; **c.** Documents approved configuration-controlled changes to the system; **d.** Retains and reviews records of configuration-controlled changes to the system; **e.** Audits activities associated with configuration-controlled changes to the system; and **f.** Coordinates and provides oversight for configuration change control activities through *a JAB approved and accepted service provider defined change control element and frequency or conditions under which it is convened. The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB.*

CM-3	**Configuration Change Control**
	g. [*Assignment: organization-defined configuration change control element*] that convenes [Selection: (one or more): [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].
Control Enhancements:	**2.** The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.
References:	• NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems.*
CM-4	**Security Impact Analysis**
Control Requirement:	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.
References:	• NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems.*
CM-5	**Access Restrictions for Change**
Control Requirement:	The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.
Control Enhancements:	**1.** The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. **5.** The organization: **(a)** Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and **(b)** Reviews and reevaluates information system developer/integrator privileges *at least quarterly*.
References:	
CM-6	**Configuration Settings**
Control Requirement:	The organization: **a.** Establishes and documents mandatory configuration settings for information technology products employed within the information system using *the United States Government Configuration Baseline (USGCB) security configuration checklists* that reflect the most restrictive mode consistent with the sensitivity level*. If USGCB security configuration checklists are not available, the service provider shall use JAB approved and accepted configuration settings based on industry best*

CM-6	**Configuration Settings**
	practices such as Center for Internet Security guidelines (Level 1) or own configuration settings. The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible if validated checklists are not available; **b.** Implements the configuration settings; **c.** Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and **d.** Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.
Control Enhancements:	**1.** The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. **3.** The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.
References:	• OMB Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*. • OMB Memorandum 07-18, *Ensuring New Acquisitions Include Common Security Configurations*. • OMB Memorandum 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)* • NIST SP 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers.* • NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems.* • Web: web.nvd.nist.gov/view/ncp/repository, National Checklist Program Repository. • Web: www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml, NSA Security Configuration Guides.
CM-7	**Least Functionality**
Control Requirement:	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services based on the *United States Government Configuration Baseline (USGCB). If USGCB security configuration checklists are not available, the service provider shall use a JAB approved and accepted list of prohibited or restricted functions, ports,*

CM-7	**Least Functionality**
	protocols, and/or services based on the Center for Internet Security guidelines (Level 1) or own list of prohibited or restricted functions, ports, protocols, and/or services.
Control Enhancements:	**1.** The organization reviews the information system *at least quarterly* to identify and eliminate unnecessary functions, ports, protocols, and/or services.
References:	
CM-8	**Information System Component Inventory**
Control Requirement:	The organization develops, documents, and maintains an inventory of information system components that: **a.** Accurately reflects the current information system; **b.** Is consistent with the authorization boundary of the information system; **c.** Is at the level of granularity deemed necessary for tracking and reporting; **d.** Includes *JAB approved and accepted service provider defined information deemed necessary to achieve effective property accountability*; and **e.** Is available for review and audit by designated organizational officials.
Control Enhancements:	**1.** The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. **3.** The organization: **a.** Employs automated mechanisms *continuously, using automated mechanisms with a* maximum five-minute *delay in detection* to detect the addition of unauthorized components/devices into the information system; and **b.** Disables network access by such components/devices or notifies designated organizational officials. **5.** The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.
References:	• NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems.*
CM-9	**Configuration Management Plan**
Control Requirement:	The organization develops, documents, and implements a configuration management plan for the information system that:

CM-9	**Configuration Management Plan**
	a. Addresses roles, responsibilities, and configuration management processes and procedures; **b.** Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and **c.** Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
References:	• NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems.*

Contingency Planning (CP)

CP-1	**Contingency Planning Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
References:	• Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements.* • NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*

CP-2	**Contingency Plan**
Control Requirement:	The organization: **a.** Develops a contingency plan for the information system that: – Identifies essential missions and business functions and associated contingency requirements; – Provides recovery objectives, restoration priorities, and metrics; – Addresses contingency roles, responsibilities, assigned individuals with contact information; – Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

CP-2 **Contingency Plan**

- – Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
- – Is reviewed and approved by designated officials within the organization.

b. Distributes copies of the contingency plan to *service provider defined key contingency personnel (identified by name and/or by role) and organizational elements that includes designated FedRAMP personnel*;

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system *at least annually*;

e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and

f. Communicates contingency plan changes to *service provider defined key contingency personnel (identified by name and/or by role) and organizational elements that includes designated FedRAMP personnel*.

Control Enhancements:

1. The organization coordinates contingency plan development with organizational elements responsible for related plans.

2. The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

References:

- Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*.
- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*.

CP-3 **Contingency Training**

Control Requirement: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training *at least annually*.

References:

- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.*
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program.*

CP-4	**Contingency Plan Testing and Exercises**
Control Requirement:	The organization: **a.** Tests and/or exercises the contingency plan using JAB approved *and accepted service provider* test plans developed in accordance with NIST Special Publication 800-34 (as amended) and provided to FedRAMP prior to testing the information system at least annually for moderate-impact systems and every three years for low-impact systems using functional exercises for moderate-impact systems and classroom exercises for low-impact systems to determine the plan's effectiveness and the organization's readiness to execute the plan; and **b.** Reviews the contingency plan test/exercise results and initiates corrective actions.
Control Enhancements:	**1.** The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems.* • NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.*
CP-6	**Alternate Storage Site**
Control Requirement:	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.
Control Enhancements:	**1.** The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. **3.** The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
References:	• NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems.*
CP-7	**Alternate Processing Site**
Control Requirement:	The organization: **a.** Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions

CP-7	**Alternate Processing Site**
	within *a JAB approved and accepted service provider defined time period consistent with the recovery time objectives and business impact analysis* when the primary processing capabilities are unavailable; and **b.** Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.
Control Enhancements:	**1.** The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards. **2.** The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. **3.** The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. **5.** The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.
References:	• NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems.*
CP-8	**Telecommunications Services**
Control Requirement:	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within *a JAB approved and accepted service provider defined time period consistent with the business impact analysis* when the primary telecommunications capabilities are unavailable.
Control Enhancements:	**1.** The organization: **a.** Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and **b.** Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

CP-8	**Telecommunications Services**
	2. The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.
References:	• NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems.* • National Communications Systems Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*. • Web: tsp.ncs.gov, *Telecommunications Service Priority (TSP) Program.*
CP-9	**Information System Backup**
Control Requirement:	The organization: **a.** Conducts backups of user-level information contained in the information system at least *daily incremental and weekly full and maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative approved and accepted by the JAB*; **b.** Conducts backups of system-level information contained in the information system at least *daily incremental and weekly full and maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative approved and accepted by the JAB*; **c.** Conducts backups of information system documentation including security-related documentation at least *daily incremental and weekly full and at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative approved and accepted by the JAB*; and The service provider shall determine what elements of the cloud environment require the Information System Backup control. The cloud environment elements requiring Information System Backup are approved and accepted by the JAB. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check. The verification and periodicity of the Information System Backup are approved and accepted by the JAB.

CP-9	**Information System Backup**
	1. The organization tests backup information *at least annually* to verify media reliability and information integrity. **3.** The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.
References:	• NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems.*

CP-10	**Information System Recovery and Reconstitution**
Control Requirement:	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
Control Enhancements:	**2.** The information system implements transaction recovery for systems that are transaction-based. **3.** The organization provides compensating security controls for *service provider defined circumstances that can inhibit recovery and reconstitution to a known state in accordance with the contingency plan for the information system and business impact analysis*.
References:	• NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*.

Identification and Authentication (IA)

IA-1	**Identification and Authentication Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
References:	• FIPS Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* • NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-63, *Electronic Authentication Guideline.*

IA-1	**Identification and Authentication Policy and Procedures**
	• NIST SP 800-73, *Interfaces for Personal Identity Verification (4 Parts)—Pt. 1- End Point PIV Card Application Namespace, Data Model & Representation; Pt. 2- PIV Card Application Card Command Interface; Pt. 3- PIV Client Application Programming Interface; Pt. 4- The PIV Transitional Interfaces & Data Model Specification.* • NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification.* • NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal NIST SP 800-100, Information Security Handbook: A Guide for Managers.*
IA-2	**Identification and Authentication (Organizational Users)**
Control Requirement:	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
Control Enhancements:	**1.** The information system uses multifactor authentication for network access to privileged accounts. **2.** The information system uses multifactor authentication for network access to non-privileged accounts. **3.** The information system uses multifactor authentication for local access to privileged accounts. **8.** The information system uses *JAB approved and accepted service provider defined replay-resistant authentication mechanisms* for network access to privileged accounts.
References:	• HSPD 12, *Policies for a Common Identification Standard for Federal Employees and Contractors.* • OMB Memorandum 04-04, *E-Authentication Guidance for Federal Agencies.* • FIPS Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* • NIST SP 800-63, *Electronic Authentication Guideline.* • NIST SP 800-73, *Interfaces for Personal Identity Verification (4 Parts)—Pt. 1- End Point PIV Card Application Namespace, Data Model & Representation; Pt. 2- PIV Card Application Card Command Interface; Pt. 3- PIV Client Application Programming Interface; Pt. 4- The PIV Transitional Interfaces & Data Model Specification.* • NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification.* • NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal.*

IA-3	**Device Identification and Authentication**
Control Requirement:	The information system uniquely identifies and authenticates before establishing a connection to *a JAB approved and accepted service provider defined list of specific devices and/or types of devices*.
References:	
IA-4	**Identifier Management**
Control Requirement:	The organization manages information system identifiers for users and devices by: **a.** Receiving authorization from a designated organizational official to assign a user or device identifier; **b.** Selecting an identifier that uniquely identifies an individual or device; **c.** Assigning the user identifier to the intended party or the device identifier to the intended device; **d.** Preventing reuse of user or device identifiers for *at least two years*; and **e.** Disabling the user identifier after *ninety days for user identifiers and a JAB approved and accepted service provider defined time period of inactivity for device identifiers*.
Control Enhancements:	**4.** The organization manages user identifiers by uniquely identifying the user as *contractors and foreign nationals*.
References:	• FIPS Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* • NIST SP 800-73, *Interfaces for Personal Identity Verification (4 Parts)—Pt. 1- End Point PIV Card Application Namespace, Data Model & Representation; Pt. 2- PIV Card Application Card Command Interface; Pt. 3- PIV Client Application Programming Interface; Pt. 4- The PIV Transitional Interfaces & Data Model Specification.* • NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification.* • NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV).*
IA-5	**Authenticator Management**
Control Requirement:	The organization manages information system authenticators for users and devices by: **a.** Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;

IA-5	**Authenticator Management**
	b. Establishing initial authenticator content for authenticators defined by the organization; **c.** Ensuring that authenticators have sufficient strength of mechanism for their intended use; **d.** Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; **e.** Changing default content of authenticators upon information system installation; **f.** Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); **g.** Changing/refreshing authenticators at least every *sixty days*; **h.** Protecting authenticator content from unauthorized disclosure and modification; and **i.** Requiring users to take, and having devices implement, specific measures to safeguard authenticators.
Control Enhancements:	**1.** The information system, for password-based authentication: **a.** Enforces minimum password complexity of *case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters;* **b.** Enforces at least *one or as determined by the information (where possible) when new passwords are created;* **c.** Encrypts passwords in storage and in transmission; **d.** Enforces password minimum and maximum lifetime restrictions of *one day minimum, sixty days maximum;* and **e.** Prohibits password reuse for *twenty four* generations. **2.** The information system, for PKI-based authentication: **(a)** Validates certificates by constructing a certification path with status information to an accepted trust anchor; **(b)** Enforces authorized access to the corresponding private key; and **(c)** Maps the authenticated identity to the user account. **3.** The organization requires that the registration process to receive *HSPD-12 smart cards* be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

IA-5	**Authenticator Management**
	6. The organization protects authenticators commensurate with the classification or sensitivity of the information accessed. **7.** The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.
References:	• OMB Memorandum 04-04, *E-Authentication Guidance for Federal Agencies.* • FIPS Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* • NIST SP 800-63, *Electronic Authentication Guideline.* • NIST SP 800-73, *Interfaces for Personal Identity Verification (4 Parts)—Pt. 1- End Point PIV Card Application Namespace, Data Model & Representation; Pt. 2- PIV Card Application Card Command Interface; Pt. 3- PIV Client Application Programming Interface; Pt. 4- The PIV Transitional Interfaces & Data Model Specification.* • NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification.* • NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV).*
IA-6	**Authenticator Feedback**
Control Requirement:	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
References:	
IA-7	**Cryptographic Module Authentication**
Control Requirement:	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
References:	• FIPS Publication 140-2, *Security Requirements for Cryptographic Modules.* • Web: csrc.nist.gov/groups/STM/cmvp/index.html.

IA-8	**Identification and Authentication (Non-Organizational Users)**
Control Requirement:	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
References:	• OMB Memorandum 04-04, *E-Authentication Guidance for Federal Agencies.* • Web: www.idmanagement.gov. • NIST SP 800-63, *Electronic Authentication Guideline*.

Incident Response (IR)

IR-1	**Incident Response Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/ updates *at least annually*: **a.** A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-61, *Computer Security Incident Handling Guide.* • NIST SP 800-83, *Guide to Malware Incident Prevention and Handling.* • NIST SP 800-100, *Information Security Handbook: |A Guide for Managers.*

IR-2	**Incident Response Training**
Control Requirement:	The organization: **a.** Trains personnel in their incident response roles and responsibilities with respect to the information system; and **b.** Provides refresher training *at least annually*.
References:	• NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* • NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program.*

IR-3	**Incident Response Testing and Exercises**
Control Requirement:	The organization tests and/or exercises the incident response capability for the information system *annually* using *tests and/or exercises in JAB approved and accepted service provider defined test plans provided to FedRAMP annually and developed in accordance with NIST Special Publication 800-61 (as amended) prior to commencing to determine the incident response effectiveness and documents the results*.
References:	• NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.* • NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment.*
IR-4	**Incident Handling**
Control Requirement:	The organization: **a.** Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; **b.** Coordinates incident handling activities with contingency planning activities; and **c.** Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. *The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.*
Control Enhancements:	**1.** The organization employs automated mechanisms to support the incident handling process.
References:	• NIST SP 800-61, *Computer Security Incident Handling Guide.*
IR-5	**Incident Monitoring**
Control Requirement:	The organization tracks and documents information system security incidents.
References:	• NIST SP 800-61, *Computer Security Incident Handling Guide.*

IR-6	**Incident Reporting**
Control Requirement:	The organization: **a.** Requires personnel to report suspected security incidents to the organizational incident response capability within *US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)*; and **b.** Reports security incident information to designated authorities.
Control Enhancements:	**1.** The organization employs automated mechanisms to assist in the reporting of security incidents.
References:	• NIST SP 800-61, *Computer Security Incident Handling Guide.* • Web: www.us-cert.gov.
IR-7	**Incident Response Assistance**
Control Requirement:	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.
Control Enhancements:	**1.** The organization employs automated mechanisms to increase the availability of incident response-related information and support. **2.** The organization: **a.** Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and **b.** Identifies organizational incident response team members to the external providers.
References:	
IR-8	**Incident Response Plan**
Control Requirement:	The organization: **a.** Develops an incident response plan that: – Provides the organization with a roadmap for implementing its incident response capability; – Describes the structure and organization of the incident response capability; – Provides a high-level approach for how the incident response capability fits into the overall organization; – Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; – Defines reportable incidents;

IR-8	**Incident Response Plan**
	– Provides metrics for measuring the incident response capability within the organization; – Defines the resources and management support needed to effectively maintain and mature an incident response capability; and – Is reviewed and approved by designated officials within the organization; **b.** Distributes copies of the incident response plan to *a service provider defined list of incident response personnel (identified by name and/or by role) and organizational element that includes designated FedRAMP personnel*; **c.** Reviews the incident response plan *at least annually*; **d.** Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and **e.** Communicates incident response plan changes to a *service provider defined list of incident response personnel (identified by name and/or by role) and organizational element that includes designated FedRAMP personnel.*
References:	• NIST SP 800-61, Computer Security Incident Handling Guide.

Maintenance (MA)

MA-1	**System Maintenance Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*

MA-2	**Controlled Maintenance**
Control Requirement:	The organization: **a.** Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; **b.** Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; **c.** Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; **d.** Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and **e.** Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
Control Enhancements:	**1.** The organization maintains maintenance records for the information system that include: **a.** Date and time of maintenance; **b.** Name of the individual performing the maintenance; **c.** Name of escort, if necessary; **d.** A description of the maintenance performed; and **e.** A list of equipment removed or replaced (including identification numbers, if applicable).
References:	
MA-3	**Maintenance Tools**
Control Requirement:	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.
Control Enhancements:	**1.** The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. **2.** The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system. **3.** The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining

MA-3	**Maintenance Tools**
	an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.
References:	• NIST SP 800-88, Guidelines for Media Sanitization.
MA-4	**Non-Local Maintenance**
Control Requirement:	The organization: **a.** Authorizes, monitors, and controls non-local maintenance and diagnostic activities; **b.** Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; **c.** Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; **d.** Maintains records for non-local maintenance and diagnostic activities; and **e.** Terminates all sessions and network connections when non-local maintenance is completed.
Control Enhancements:	**1.** The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions. **2.** The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.
References:	• FIPS Publications 140-2, *Security Requirements for Cryptographic Modules.* • FIPS Publications 197, *Advanced Encryption Standard.* • FIPS Publications 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* • NIST SP 800-63, *Electronic Authentication Guideline.* • NIST SP 800-88, *Guidelines for Media Sanitization.* • CNSS Policy 15, *National Policy on the Use of the Advanced Encryption (AES) to Protect National Security Systems and National Security Information.*
MA-5	**Maintenance Personnel**
Control Requirement:	The organization: **a.** Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and

MA-5	**Maintenance Personnel**
	b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
References:	
MA-6	**Timely Maintenance**
Control Requirement:	The organization obtains maintenance support and/or spare parts for *a JAB approved and accepted service provider defined list of security-critical information system components and/or key information technology components* within *a JAB approved and accepted service provider defined time period* of failure *to obtain maintenance and spare parts that is in a accordance with the contingency plan for the information system and business impact analysis*.
References:	

Media Protection (MP)

MP-1	**Media Protection Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*
MP-2	**Media Access**
Control Requirement:	The organization restricts access to *a JAB approved and accepted service provider defined types of digital and non-digital media* to *a JAB approved and accepted service provider defined list of individuals with authorized access to the media types* using *JAB approved and accepted service provider defined types of security measures to be used in protecting the media types*.

MP-2	**Media Access**
Control Enhancements:	**1.** The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices.*
MP-3	**Media Markings**
Control Requirement:	The organization: **a.** Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and **b.** Exempts *no removable media types* from marking.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.*
MP-4	**Media Storage**
Control Requirement:	The organization: **a.** Physically controls and securely stores *magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks within service provider defined controlled areas within facilities where the information and information system resides using encryption with FIPS 140-2 validated encryption modules for digital media and secure storage in locked cabinets and safes for non-digital media; and* **b.** Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
Control Enhancements:	**1.** The organization employs cryptographic mechanisms to protect information in storage.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-56 (A, B, and C), *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography; Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography; Recommendation for Key Derivation through Extraction-then-Expansion.*

MP-4	**Media Storage**
	• NIST SP 800-57, *Recommendation for Key Management.* • NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices.*
MP-5	**Media Transport**
Control Requirement:	The organization: **a.** Protects and controls *magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks* during transport outside of controlled areas using *encryption with FIPS 140-2 validated encryption modules for digital media, and a JAB approved and accepted service provider defined security measures to protect digital and non-digital media, and JAB approved and accepted service provider defined security measures to protect digital and non-digital media in transport;* **b.** Maintains accountability for information system media during transport outside of controlled areas; and **c.** Restricts the activities associated with transport of such media to authorized personnel.
Control Enhancements:	**2.** The organization documents activities associated with the transport of information system media. **4.** The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)—Volume 1: Guide Volume 2: Appendices.*
MP-6	**Media Sanitization**
Control Requirement:	The organization: **a.** Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and **b.** Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

MP-6	**Media Sanitization**
Control Enhancements:	**4.** The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)—Volume 1: Guide Volume 2: Appendices.* • NIST SP 800-88, *Guidelines for Media Sanitization.* • Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml, *Media Destruction Guidance.*

Physical and Environmental Protection (PE)

PE-1	**Physical and Environmental Protection Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*

PE-2	**Physical Access Authorizations**
Control Requirement:	The organization: **a.** Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

PE-2	**Physical Access Authorizations**
	b. Issues authorization credentials; and **c.** Reviews and approves the access list and authorization credentials *at least annually*, removing from the access list personnel no longer requiring access.
References:	
PE-3	**Physical Access Control**
Control Requirement:	The organization: **a.** Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); **b.** Verifies individual access authorizations before granting access to the facility; **c.** Controls entry to the facility containing the information system using physical access devices and/or guards; **d.** Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; **e.** Secures keys, combinations, and other physical access devices; **f.** Inventories physical access devices *at least annually* and **g.** Changes combinations and keys *at least annually* and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
References :	• FIPS Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* • NIST SP 800-73, *Interfaces for Personal Identity Verification (4 Parts)—Pt. 1- End Point PIV Card Application Namespace, Data Model & Representation; Pt. 2- PIV Card Application Card Command Interface; Pt. 3- PIV Client Application Programming Interface; Pt. 4- The PIV Transitional Interfaces & Data Model Specification.* • NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification.* • NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV).*

PE-3	**Physical Access Control**
	• ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access and other Controlled Access Program Information to Sensitive Compartmented Information.* • DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities.*
PE-4	**Access Control for Transmission Medium**
Control Requirement:	The organization controls physical access to information system distribution and transmission lines within organizational facilities.
References:	• NSTISSI No. 7003, P*rotective Distribution Systems (PDS).*
PE-5	**Access Control for Output Devices**
Control Requirement:	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
References:	
PE-6	**Monitoring Physical Access**
Control Requirement:	The organization: **a.** Monitors physical access to the information system to detect and respond to physical security incidents; **b.** Reviews physical access logs *at least semi-annually*; and **c.** Coordinates results of reviews and investigations with the organization's incident response capability.
Control Enhancements:	**1.** The organization monitors real-time physical intrusion alarms and surveillance equipment.
References:	
PE-7	**Visitor Control**
Control Requirement:	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
Control Enhancements:	**1.** The organization escorts visitors and monitors visitor activity, when required.
References:	

PE-8	**Access Records**
Control Requirement:	The organization: **a.** Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and **b.** Reviews visitor access records *at least monthly*.
References:	
PE-9	**Power Equipment and Power Cabling**
Control Requirement:	The organization protects power equipment and power cabling for the information system from damage and destruction.
References:	
PE-10	**Emergency Shutoff**
Control Requirement:	The organization: **a.** Provides the capability of shutting off power to the information system or individual system components in emergency situations; **b.** Places emergency shutoff switches or devices in *JAB approved and accepted service provider defined emergency shutoff switch locations* by information system or system component, to facilitate safe and easy access for personnel; and **c.** Protects emergency power shutoff capability from unauthorized activation.
References:	
PE-11	**Emergency Power**
Control Requirement:	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.
References:	
PE-12	**Emergency Lighting**
Control Requirement:	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
References:	
PE-13	**Fire Protection**
Control Requirement:	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

PE-13 **Fire Protection**

Control Enhancements:

1. The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.
2. The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.
3. The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

References:

PE-14 **Temperature and Humidity Controls**

Control Requirement: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides consistent with *American Society of Heating, Refrigerating and Air-conditioner Engineers (ASHRAE) document entitled Thermal Guidelines for Data Processing Environments and measures temperature at server inlets and humidity levels by dew point;* and

b. Monitors temperature and humidity levels *continuously.*

References:

PE-15 **Water Damage Protection**

Control Requirement: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

References:

PE-16 **Delivery and Removal**

Control Requirement: The organization authorizes, monitors, and controls *all information system components* entering and exiting the facility and maintains records of those items.

References:

PE-17 **Alternate Work Site**

Control Requirement: The organization:

a. Employs control requirements, as per *JAB approved and accepted service provider defined management, operational, and technical information system security controls* at alternate work sites;

PE-17	Alternate Work Site
	b. Assesses, as feasible, the effectiveness of security controls at alternate work sites; and **c.** Provides a means for employees to communicate with information security personnel in case of security incidents or problems.
References:	• NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security.*

PE-18	Location of Information System Components
Control Requirement:	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.
References:	

Planning (PL)

PL-1	Security Planning Policy and Procedures
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*

PL-2	System Security Plan
Control Requirement:	The organization: **a.** Develops a security plan for the information system that: – Is consistent with the organization’s enterprise architecture; – Explicitly defines the authorization boundary for the system; – Describes the operational context of the information system in terms of missions and business processes; – Provides the security categorization of the information system including supporting rationale; – Describes the operational environment for the information system; – Describes relationships with or connections to other information systems;

PL-2	**System Security Plan**
	– Provides an overview of the security requirements for the system; – Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and – Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; **b.** Reviews the security plan for the information system *at least annually*; and **c.** Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
References:	• NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems.*
PL-4	**Rules of Behavior**
Control Requirement:	The organization: **a.** Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and **b.** Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
References:	• NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems.*
PL-5	**Privacy Impact Assessment**
Control Requirement:	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.
References:	• OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
PL-6	**Security-Related Activity Planning**
Control Requirement:	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.
References:	

Personnel Security (PS)

PS-1	**Personnel Security Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*
PS-2	**Position Categorization**
Control Requirement:	The organization: **a.** Assigns a risk designation to all positions; **b.** Establishes screening criteria for individuals filling those positions; and **c.** Reviews and revises position risk designations *at least every three years*.
References:	• C.F.R. 731.106(a), *Designation of Public Trust Positions and Investigative Requirements—Risk Designation.*
PS-3	**Personnel Screening**
Control Requirement:	The organization: **a.** Screens individuals prior to authorizing access to the information system; and **b.** Rescreens individuals according to the following conditions: *For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance.* *For moderate-risk law enforcement and high-impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate-risk positions or any low-risk positions.*

PS-3	**Personnel Screening**
References:	• 5 C.F.R. 731.106, *Designation of Public Trust Positions and Investigative Requirements.* • FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • FIPS Publications 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* • NIST SP 800-73, *Interfaces for Personal Identity Verification (4 Parts)—Pt. 1- End Point PIV Card Application Namespace, Data Model & Representation; Pt. 2- PIV Card Application Card Command Interface; Pt. 3- PIV Client Application Programming Interface; Pt. 4- The PIV Transitional Interfaces & Data Model Specification.* • NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification.* • NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access and Other Controlled Access Program Information to Sensitive Compartmented Information.*
PS-4	**Personnel Termination**
Control Requirement:	The organization, upon termination of individual employment: **a.** Terminates information system access; **b.** Conducts exit interviews; **c.** Retrieves all security-related organizational information and system-related property; and **d.** Retains access to organizational information and information systems formerly controlled by terminated individual.
References:	
PS-5	**Personnel Transfer**
Control Requirement:	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates *JAB approved and accepted service provider defined transfer or reassignment actions* within *five days*.
References:	

PS-6	**Access Agreements**
Control Requirement:	The organization: **a.** Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and **b.** Reviews/updates the access agreements *at least annually*.
References:	

PS-7	**Third-Party Personnel Security**
Control Requirement:	The organization: **a.** Establishes personnel security requirements including security roles and responsibilities for third-party providers; **b.** Documents personnel security requirements; and **c.** Monitors provider compliance.
References:	• NIST SP 800-35, *Guide to Information Technology Security Services.*

PS-8	**Personnel Sanctions**
Control Requirement:	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
References:	

Risk Assessment (RA)

RA-1	**Risk Assessment Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-30, *Guide for Conducting Risk Assessments.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*

RA-2	**Security Categorization**
Control Requirement:	The organization: **a.** Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; **b.** Documents the security categorization results (including supporting rationale) in the security plan for the information system; and **c.** Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official-designated representative.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-30, *Guide for Conducting Risk Assessments.* • NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View.* • NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)—Volume 1: Guide Volume 2: Appendices.*
RA-3	**Risk Assessment**
Control Requirement:	The organization: **a.** Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; **b.** Documents risk assessment results in *security assessment report*; **c.** Reviews risk assessment results *at least every three years or when a significant change occurs*; and **d.** Updates the risk assessment *at least every three year* or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
References:	• NIST SP 800-30, *Guide for Conducting Risk Assessments.* • NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View.*

RA-5	**Vulnerability Scanning**
Control Requirement:	The organization: **a.** Scans for vulnerabilities in the information system and hosted applications *monthly operating system/infrastructure, quarterly web applications and databases, an accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually*, and when new vulnerabilities potentially affecting the system/applications are identified and reported; **b.** Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: – Enumerating platforms, software flaws, and improper configurations; – Formatting and making transparent, checklists and test procedures; and – Measuring vulnerability impact; **c.** Analyzes vulnerability scan reports and results from security control assessments; **d.** Remediates legitimate vulnerabilities *high-risk vulnerabilities mitigated within thirty days, moderate risk vulnerabilities mitigated within ninety days,* in accordance with an organizational assessment of risk; and **e.** Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
Control Enhancements:	**1.** The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. **2.** The organization updates the list of information system vulnerabilities scanned *continuously, before each scan* or when new vulnerabilities are identified and reported. **3.** The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

RA-5	**Vulnerability Scanning**
Control Enhancements:	**5.** The organization includes privileged access authorization to *operating systems/infrastructure, databases, web applications* for selected vulnerability scanning activities to facilitate more thorough scanning. **6.** The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. **9.** The organization employs an independent penetration agent or penetration team to: **a.** Conduct a vulnerability analysis on the information system; and **b.** Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.
References:	• NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*. • NIST SP 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*. • NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*. • Web: cwe.mitre.org, *Common Weakness Enumeration*. • Web: nvd.nist.gov, *National Vulnerability Database.*

System and Services Acquisition (SA)

SA-1	**System and Services Acquisition Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*

SA-2	**Allocation of Resources**
Control Requirement:	The organization: **a.** Includes a determination of information security requirements for the information system in mission/business process planning; **b.** Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and **c.** Establishes a discrete line item for information security in organizational programming and budgeting documentation.
References:	• NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process.*

SA-3	**Life Cycle Support**
Control Requirement:	The organization: **a.** Manages the information system using a system development life cycle methodology that includes information security considerations; **b.** Defines and documents information system security roles and responsibilities throughout the system development life cycle; and **c.** Identifies individuals having information system security roles and responsibilities.
References:	• NIST SP 800-64, *Security Considerations in the System Development Life Cycle.*

SA-4	**Acquisitions**
Control Requirement:	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: **a.** Security functional requirements/specifications; **b.** Security-related documentation requirements; and **c.** Developmental and evaluation-related assurance requirements.
Control Enhancements:	**1.** The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.

SA-4	**Acquisitions**
	4. The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment. **7.** The organization: **a.** Limits the use of commercially provided information technology products to those products that have been successfully evaluated against a validated US Government Protection Profile for a specific technology type, if such a profile exists; and **b.** Requires, if no US Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, then the cryptographic module is FIPS-validated.
References:	• ISO/IEC 15408, *Information technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model.* • FIPS 140-2, *Security Requirements for Cryptographic Modules.* • NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products.* • NIST SP 800-35, *Guide to Information Technology Security Services.* • NIST SP 800-36, *Guide to Selecting Information Technology Security Products.* • NIST SP 800-64, *Security Considerations in the System Development Life Cycle.* • NIST SP 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers.* • Web: www.niap-ccevs.org, *The Common Criteria Evaluation and Validation Scheme*.
SA-5	**Information System Documentation**
Control Requirement:	The organization: **a.** Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: – Secure configuration, installation, and operation of the information system;

SA-5	Information System Documentation
	– Effective use and maintenance of security features/functions; and – Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and **b.** Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: – User-accessible security features/functions and how to effectively use those security features/functions; – Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and – User responsibilities in maintaining the security of the information and information system; and **c.** Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.
Control Enhancements:	**1.** The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing. **3.** The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.
References:	
SA-6	**Software Usage Restrictions**
Control Requirement:	The organization: **a.** Uses software and associated documentation in accordance with contract agreements and copyright laws; **b.** Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and **c.** Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
References:	

SA-7	**User-Installed Software**
Control Requirement:	The organization enforces explicit rules governing the installation of software by users.
References:	
SA-8	**Security Engineering Principles**
Control Requirement:	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.
References:	• NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security).*
SA-9	**External Information System Services**
Control Requirement:	The organization: **a.** Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; **b.** Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and **c.** Monitors security control compliance by external service providers.
Control Enhancements:	**1.** The organization: **a.** Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and **b.** Ensures that the acquisition or outsourcing of dedicated information security services is approved by *the Joint Authorization Board (JAB)*. *The service provider documents all existing outsourced security services and conducts a risk assessment of future outsourced security services. Future, planned outsourced services are approved and accepted by the JAB*.
References:	• NIST SP 800-35, G*uide to Information Technology Security Services.*
SA-10	**Developer Configuration Management**
Control Requirement:	The organization requires that information system developers/ integrators: **a.** Perform configuration management during information system design, development, implementation, and operation;

SA-10	**Developer Configuration Management**
	b. Manage and control changes to the information system; **c.** Implement only organization-approved changes; **d.** Document approved changes to the information system; and **e.** Track security flaws and flaw resolution.
References:	

SA-11	**Developer Security Testing**
Control Requirement:	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): **a.** Create and implement a security test and evaluation plan; **b.** Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and **c.** Document the results of the security testing/evaluation and flaw remediation processes.
Control Enhancements:	**1.** The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis. *The service provider submits a code analysis report as part of the authorization package and updates the report in any reauthorization actions. The service provider documents in the Continuous Monitoring Plan how newly developed code for the information system is reviewed*.
References:	

SA-12	**Supply Chain Protection**
Control Requirement:	The organization protects against supply chain threats by employing: *JAB approved and accepted service provider defined list of measures to protect against supply chain threats* as part of a comprehensive, defense-in-breadth information security strategy.
References:	

System and Communications Protection (SC)

SC-1	**System and Communications Protection Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

SC-1	**System and Communications Protection Policy and Procedures**
	b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*
SC-2	**Application Partitioning**
Control Requirement:	The information system separates user functionality (including user interface services) from information system management functionality.
References:	
SC-4	**Information in Shared Resources**
Control Requirement:	The information system prevents unauthorized and unintended information transfer via shared system resources.
References:	
SC-5	**Denial of Service Protection**
Control Requirement:	The information system protects against or limits the effects of the following types of denial of service attacks: *a JAB approved and accepted service provider defined list of denial of service attack types (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list.*
References:	
SC-6	**Resource Priority**
Control Requirement:	The information system limits the use of resources by priority.
References:	
SC-7	**Boundary Protection**
Control Requirement:	The information system: **a.** Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and **b.** Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

SC-7	Boundary Protection
Control Enhancements:	1. The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. *The service provider and service consumer ensure that federal information (other than unrestricted information) being transmitted from federal government entities to external entities using information systems providing cloud services is inspected by TIC processes.* 2. The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. 3. The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. 4. The organization: a. Implements a managed interface for each external telecommunication service; b. Establishes a traffic flow policy for each managed interface; c. Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; d. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; e. Reviews exceptions to the traffic flow policy *at least annually*; and f. Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. 5. The information system, at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). 7. The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. 8. The information system routes *JAB approved and accepted service provider defined internal communications traffic to JAB approved and accepted external networks that are the prospective destination of such traffic routing* through authenticated proxy servers within the managed interfaces of boundary protection devices. 12. The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.

SC-7	**Boundary Protection**
	13. The organization isolates *service provider defined key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components* from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.
	18. The information system fails securely in the event of an operational failure of a boundary protection device.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* • NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy.* • NIST SP 800-77, *Guide to IPsec VPNs.*
SC-8	**Transmission Integrity**
Control Requirement:	The information system protects the integrity of transmitted information.
Control Enhancements:	1. The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.
References:	• FIPS Publications 140-2, *Security Requirements for Cryptographic Modules.* • FIPS Publications 197, *Advanced Encryption Standard.* • NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations.* • NIST SP 800-77, *Guide to IPsec VPNs.* • NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide.* • NIST SP 800-113, *Guide to SSL VPNs.* • NSTISSI No. 7003, *Protective Distribution Systems (PDS).*
SC-9	**Transmission Confidentiality**
Control Requirement:	The information system protects the confidentiality of transmitted information.
Control Enhancements:	1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by *implementing a hardened or alarmed carrier Protective Distribution System (PDS) when transmission confidentiality cannot be achieved through cryptographic mechanisms*.

SC-9	**Transmission Confidentiality**
References:	• FIPS Publications 140-2, *Security Requirements for Cryptographic Modules.* • FIPS Publications 197, *Advanced Encryption Standard.* • NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations.* • NIST SP 800-77, *Guide to IPsec VPNs.* • NIST SP 800-113, *Guide to SSL VPNs.* • CNSS Policy 15, *National Policy on the Use of the Advanced Encryption Standards (AES) to Protect National Security Systems and National Security Information.* • NSTISSI No. 7003, *Protective Distribution Systems (PDS).*
SC-10	**Network Disconnect**
Control Requirement:	The information system terminates the network connection associated with a communications session at the end of the session or after *thirty minutes for all RAS-based sessions and thirty to sixty minutes for non-interactive users* of inactivity.
References:	
SC-11	**Trusted Path**
Control Requirement:	The information system establishes a trusted communications path between the user and the following security functions of the system: *JAB approved and accepted service provider defined list of security functions that require a trusted path, including but not limited to system authentication, re-authentication and provisioning or de-provisioning of services (i.e., allocating additional bandwidth to a cloud user)*.
References:	
SC-12	**Cryptographic Key Establishment and Management**
Control Requirement:	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.
Control Enhancements:	**2.** The organization produces, controls, and distributes symmetric cryptographic keys using *NIST-approved* key management technology and processes. **5.** The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key. *The service provider supports the capability to produce, control, and distribute asymmetric cryptographic keys*.

SC-12	**Cryptographic Key Establishment and Management**
References:	• NIST SP 800-56 (A, B, C), *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography; Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography; Recommendation for Key Derivation through Extraction-then-Expansion.* • NIST SP 800-57, *Recommendation for Key Management.*
SC-13	**Use of Cryptography**
Control Requirement:	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
Control Enhancements:	**1.** The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.
References:	• FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*. • Web: csrc.nist.gov/groups/STM/cmvp/index.html, *Cryptographic Module Validation Program (CMVP)*.
SC-14	**Public Access Protections**
Control Requirement:	The information system protects the integrity and availability of publicly available information and applications.
References:	
SC-15	**Collaborative Computing Devices**
Control Requirement:	The information system: **a.** Prohibits remote activation of collaborative computing devices with *no exceptions*; and **b.** Provides an explicit indication of use to users physically present at the devices. *The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.*
References:	
SC-17	**Public Key Infrastructure Certificates**
Control Requirement:	The organization issues public key certificates under a *JAB approved and accepted service provider defined public key infrastructure certificate policy* or obtains public key certificates under an appropriate certificate policy from an approved service provider.

SC-17	**Public Key Infrastructure Certificates**
References:	• OMB Memorandum 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors.* • NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure.* • NIST SP 800-63, *Electronic Authentication Guideline.*
SC-18	**Mobile Code**
Control Requirement:	The organization: **a.** Defines acceptable and unacceptable mobile code and mobile code technologies; **b.** Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and **c.** Authorizes, monitors, and controls the use of mobile code within the information system.
References:	• NIST SP 800-28, *Guidelines on Active Content and Mobile Code*. • DoD Instruction 8552.01, *Use of Mobile Code Technologies in DoD Information Systems.*
SC-19	**Voice Over Internet Protocol**
Control Requirement:	The organization: **a.** Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and **b.** Authorizes, monitors, and controls the use of VoIP within the information system.
References:	• NIST SP 800-58, *Security Considerations for Voice Over IP Systems.*
SC-20	**Secure Name/Address Resolution Service (Authoritative Source)**
Control Requirement:	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

SC-20	**Secure Name/Address Resolution Service (Authoritative Source)**
Control Enhancements:	1. The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.
References:	• OMB Memorandum 08-23, *Securing the Federal Government's Domain Name System Infrastructure.* • NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide.*
SC-21	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**
Control Requirement:	The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.
References:	• NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide.*
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**
Control Requirement:	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.
References:	• NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*.
SC-23	**Session Authenticity**
Control Requirement:	The information system provides mechanisms to protect the authenticity of communications sessions.
References:	• NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*. • NIST SP 800-77, *Guide to IPsec VPNs*. • NIST SP 800-95, *Guide to Secure Web Services*.
SC-28	**Protection of Information at Rest**
Control Requirement:	The information system protects the confidentiality and integrity of information at rest. *The organization supports the capability to use cryptographic mechanisms to protect information at rest*.

SC-28	**Protection of Information at Rest**
References:	• NIST SP 800-56, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.* • NIST SP 800-57, *Recommendation for Key Management.* • NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices.*
SC-30	**Virtualization Techniques**
Control Requirement:	The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.
References:	
SC-32	**Information System Partitioning**
Control Requirement:	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.
References:	• FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

System and Information Integrity (SI)

SI-1	**System and Information Integrity Policy and Procedures**
Control Requirement:	The organization develops, disseminates, and reviews/updates *at least annually*: **a.** A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and **b.** Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
References:	• NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook.* • NIST SP 800-100, *Information Security Handbook: A Guide for Managers.*

SI-2	**Flaw Remediation**
Control Requirement:	The organization: **a.** Identifies, reports, and corrects information system flaws; **b.** Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and **c.** Incorporates flaw remediation into the organizational configuration management process.
Control Enhancements:	**2.** The organization employs automated mechanisms *at least monthly* to determine the state of information system components with regard to flaw remediation.
References:	• NIST SP 800-40, *Creating a Patch and Vulnerability Management Program.*
SI-3	**Malicious Code Protection**
Control Requirement:	The organization: **a.** Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: – Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or – Inserted through the exploitation of information system vulnerabilities; **b.** Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; **c.** Configures malicious code protection mechanisms to: – Perform periodic scans of the information system *at least weekly* and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and – Blocks *or quarantine malicious code,* sends *alert to administrator, and* sends *an alert to FedRAMP* in response to malicious code detection; and **d.** Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

SI-3	**Malicious Code Protection**
Control Enhancements:	**1.** The organization centrally manages malicious code protection mechanisms. **2.** The information system automatically updates malicious code protection mechanisms (including signature definitions). **3.** The information system prevents non-privileged users from circumventing malicious code protection capabilities.
References:	• NIST SP 800-83, *Guide to Malware Incident Prevention and Handling.*
SI-4	**Information System Monitoring**
Control Requirement:	The organization: **a.** Monitors events on the information system to *ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise* and detects information system attacks; **b.** Identifies unauthorized use of the information system; **c.** Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; **d.** Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and **e.** Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
Control Enhancements:	**2.** The organization employs automated tools to support near real-time analysis of events. **4.** The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

SI-4	**Information System Monitoring**
	5. The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: *protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose. The service provider defines additional compromise indicators as needed*. **6.** The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.
References:	• NIST SP 800-61, *Computer Security Incident Handling Guide*. • NIST SP 800-83, *Guide to Malware Incident Prevention and Handling.* • NIST SP 800-92, *Guide to Computer Security Log Management.* • NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS).* • NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.

SI-5	**Security Alerts, Advisories, and Directives**
Control Requirement:	The organization: **a.** Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; **b.** Generates internal security alerts, advisories, and directives as deemed necessary; **c.** Disseminates security alerts, advisories, and directives to *all staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP. The service provider defines a list of personnel identified by name and/or role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives, to include designated FedRAMP personnel*; and **d.** Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
References:	• NIST SP 800-40, *Creating a Patch and Vulnerability Management Program.*
SI-6	**Security Functionality Verification**
Control Requirement:	The information system verifies the correct operation of security functions *upon system startup and/or restart and periodically every ninety days* and *notifies system administrator* when anomalies are discovered.
References:	
SI-7	**Software and Information Integrity**
Control Requirement:	The information system detects unauthorized changes to software and information.
Control Enhancements:	**1.** The organization reassesses the integrity of software and information by performing *at least monthly* integrity scans of the information system.
References:	
SI-8	**Spam Protection**
Control Requirement:	The organization: **a.** Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, or other common means; and

SI-8	**Spam Protection**
	b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.
References:	• NIST SP 800-45, *Guidelines on Electronic Mail Security.*
SI-9	**Information Input Restrictions**
Control Requirement:	The organization restricts the capability to input information to the information system to authorized personnel.
References:	
SI-10	**Information Input Verification**
Control Requirement:	The information system checks the validity of information inputs.
References:	
SI-11	**Error Handling**
Control Requirement:	The information system: **a.** Identifies potentially security-relevant error conditions; **b.** Generates error messages that provide information necessary for corrective actions without revealing *user name and password combinations; attributes used to validate a password reset request (e.g., security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g., account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes, and settings)* in error logs and administrative messages that could be exploited by adversaries; and **c.** Reveals error messages only to authorized personnel.
References:	
SI-12	**Information Output Handling and Retention**
Control Requirement:	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
References:	

SUMMARY

This chapter provided a detailed discussion of the FedRAMP security controls, including the security selection process used by the JAB. In addition, specific issues regarding to roles and responsibilities were highlighted at they relate to the delineation of responsibility for security controls and situations where shared responsibilities would require defining the scope that would need to be addressed in governing policies and procedures. The governance and maintenance of the FedRAMP security requirements were briefly discussed, focusing on the application of a harmonizing process to incorporate industry feedback and agency-specific security and privacy. Finally, the FedRAMP security control requirements were described, to include potential approaches for implementing the security controls, both in existing or new cloud services with an emphasis on applying a gap analysis or integrating them through a traditional SDLC.

References

[1] FedRAMP Program Management Office (PMO). FedRAMP security controls preface [Internet]. Washington: US General Services Administration [cited March 13, 2012]. <http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip>.

[2] Joint Task Force Transformation Initiative. Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and privacy controls for federal information system and organizations. Maryland: National Institute of Standards and Technology; 2012.

[3] FedRAMP Program Management Office (PMO). FedRAMP concept of operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012.

[4] Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 3, Recommended security controls for federal information system and organizations. Maryland: National Institute of Standards and Technology; 2010.

[5] NIST Computer Security Division, Computer Security Resource Center [Internet]. Washington: US General Services Administration [cited March 4, 2012]. <http://csrc.nist.gov/groups/SMA/fisma/index.html>.

[6] FedRAMP Program Management Office (PMO). Federal risk and authorization management program (FedRAMP), security controls briefing. Washington: US General Services Administration; 2012.

[7] E-Government Act of 2002 [Internet]. Washington: US Government Printing Office; [cited March 10, 2012]. <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.html>.

[8] US General Services Administration. FAR Subpart 7.1 [Internet]. Washington: US General Services Administration; [cited March 13, 2012]. <https://www.acquisition.gov/far/current/html/Subpart%207_1.html>.

[9] US General Services Administration. FAR Subpart 7.1 [Internet]. Washington: US General Services Administration; [cited March 13, 2012]. <https://www.acquisition.gov/far/html/Subpart%2011_1.html>.

[10] US General Services Administration. FAR Subpart 7.1 [Internet]. Washington: US General Services Administration; [cited March 13, 2012]. <https://www.acquisition.gov/far/html/Subpart%2039_1.html>.

[11] Cloud Security Alliance Working Group. Security guidance for critical areas of focus in cloud computing V3.0. Washington: Cloud Security Alliance; 2011.

[12] FedRAMP Program Management Office (PMO). FedRAMP security controls [Internet]. Washington: US General Services Administration [cited March 3, 2011]. <http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip>.

[13] US General Services Administration. FAR Subpart 7.1 [Internet]. Washington: U.S. General Services Administration [cited 2012 Mar 13]. Available from: https://www.acquisition.gov/far/html/52_233_240.html

This page is intentionally left blank

CHAPTER

Security Assessment and Authorization: Governance, Preparation, and Execution 10

INFORMATION IN THIS CHAPTER:

- Introduction to the Security Assessment Process
- Governing the Security Assessment
- Preparing for the Security Assessment
- Executing the Security Assessment Plan

INTRODUCTION TO THE SECURITY ASSESSMENT PROCESS

The security assessment process is a key component of the NIST Risk Management Framework (RMF)[1] and the Federal Risk and Authorization Management Program (FedRAMP).[2] FedRAMP[3] enables the adoption and use of cloud services through a cost-effective, risk-based approach that ensures security assessments are an integral part of the system development life cycle (SDLC).[4] FedRAMP also enables federal agencies to benefit from the application of a security risk model that allows them to leverage the authorization through a unified, consistent security assessment framework.

The goal of a security assessment is to establish confidence that the security controls employed within the information system (or those inherited) have been effectively implemented and are operating as intended. Security assessments conducted at

[1] Chapter 5 discussed the risk management activities involved in the application of the Risk Management Framework (RMF).

[2] From FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. *"A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services."*

[3] Chapter 8 discussed the FedRAMP process areas.

[4] From Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., Gulick, J. NIST Special Publication (SP) 800-64 Revision 2, Security Considerations in the System Development Life Cycle. Maryland: National Institute of Standards and Technology; 2008. *"Security planning in the initiation phase should include preparations for the entire system life cycle, including the identification of key security milestones and deliverables, and tools and technologies. Special consideration should be given to items that may need to be procured (e.g. test/assessment tools)."*

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00010-1

different stages throughout the SDLC,[5] can benefit organizations by reducing costs through the reuse of evidence produced through the design, implementation, and testing of the required security controls. By identifying the gaps in security requirements early in the SDLC process,[6] some security controls can be more cost-effectively designed and implemented within the information security architecture,[7] and tested[8] prior to being fully integrated into the production operating environment.

The authorization step relies upon the quality of the evidence and the results of the security assessment documented in the security assessment report (SAR). The SAR is one of the three key documents presented to the authorizing official (AO)[9] when making a credible, risk-based decision. The AO uses the information from the security assessment results[10] as a factor for assuming responsibility for the information systems operation and the information that will be processed, stored, or transmitted within the information system. Through an analysis of the risk associated with the weaknesses and deficiencies identified during the security assessment, the AO can use the judgment of the assessor to make a determination if they are deemed to

[5] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. "Conducting security control assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions. The results of security control assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the security authorization process to avoid system fielding delays or costly repetition of assessments."

[6] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"There are typically five phases in a generic system development life cycle: (i) initiation; (ii) development/acquisition; (iii) implementation; (iv) operations and maintenance; and (v) disposition (disposal)."*

[7] From Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., Gulick, J. NIST Special Publication (SP) 800-64 Revision 2, Security Considerations in the System Development Life Cycle. Maryland: National Institute of Standards and Technology; 2008. *"Schematic of security integration providing details on where, within the system, security is implemented and shared."*

[8] From Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., Gulick, J. NIST Special Publication (SP) 800-64 Revision 2, Security Considerations in the System Development Life Cycle. Maryland: National Institute of Standards and Technology; 2008. *For example, "testing of basic security controls during functional testing may reduce or eliminate issues earlier in the development cycle (e.g. mandatory access controls, secure code development, and firewalls)."*

[9] The FedRAMP Joint Authorization Board (JAB) only grants a provisional authorization for cloud services that have undergone a FedRAMP assessment with an accredited Third Party Assessment Organization (3PAO) which enables federal agencies to accept the risk-based decision for granting their own authorization, or federal agencies can conduct their own assessment utilizing the FedRAMP assessment process and a 3PAO for making a risk-based decision.

[10] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The results of security control assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the security authorization process."*

be acceptable. This reliance on the quality and reliability of the results of the security assessment places a significant importance on the selection of the independent security assessment provider (or security assessor).[11] The security assessment provider must be qualified and competent in conducting security assessments and capable of assessing the security controls, including compiling the evidence needed to demonstrate the effectiveness of the security controls employed within the information system. In addition the security assessor must be able to effectively present the evidence in a manner that enables a risk-based decision to be made.

In this chapter, the NIST RMF Step 4 (*Assessment*) and Step 5 (*Authorization*) steps will be discussed, with the focus on assisting organizations in developing their organization-wide strategy by presenting a framework for managing security assessments. The framework includes three key areas:

- Governance.
- Preparation.
- Execution.

NOTE

The Federal Risk and Authorization Management Program (FedRAMP) provides a structured, policy-driven process for building a trusted relationship between Cloud Service Providers (CSP) and federal agency customers. In addition, it supports the acceleration, and secure adoption and use of commercial and non-commercial cloud services through a cost-effective, risk-based approach to security authorization by integrating security assessment as a part of the system development life cycle (SDLC). FedRAMP also enables federal agencies to benefit from the application of a security risk model that allows them to leverage the authorization through a unified, consistent security assessment framework.

GOVERNANCE IN THE SECURITY ASSESSMENT

The security assessment policy establishes the governance for the security assessment process. The policy, at a minimum, should cover the requirements for the security assessment preparation and execution, the methodology by which the security assessment is directed and guided, and the roles and responsibilities. The security assessment methodology establishes a repeatable framework for conducting security assessments through the consistent and structured application of assessment procedures, processes, methods, and practices [4]. The methodology[12] also addresses the

[11] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system."*

[12] NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment,* Appendix E includes some example methodologies. Available from: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

approach the organization will use for determining the reuse of security assessment results and how the security assessment will be conducted.

There are generally two primary roles in security assessments, the *security assessment customer* and the *security assessment provider*.[13] Security assessment customers and providers can be from the same organization or the provider can be contracted from a public or private entity outside of the customer organization. However, to ensure the effectiveness and efficiency of security assessments, a degree of independence is critical, specifically for reusing previous assessment results.[14] For example, security assessment-related documentation and evidence could be produced from testing conducted as an integrated part of the SDLC[15] or from third-party testing [16] [5]"if an information system component product is identified as providing support for the implementation of a particular security control" [1].

Security assessments can also include assessment results from other security assessments performed from outside of the organization. In these situations, factors relating to the security assessment results for security controls outside of the boundary for the information system being assessed must consider the credibility of the results being inherited,[17] *partially* or *completely*, at the organization-level (i.e., information security program) rather than the information at system-level to preserve impartiality.

[13] From Joint Task Force Transformation Initiative Interagency Working Group. NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Maryland: National Institute of Standards and Technology; 2010. The security assessment provider can be an "individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e. the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system)."

[14] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. "Organizations can take advantage of previous assessment results whenever possible, to reduce the overall cost of assessments and to make the assessment process more efficient."

[15] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. Assessment results can be obtained from many activities that occur routinely during the system development life cycle to reduce the overall cost of assessments and to make the assessment process more efficient.

[16] From The Common Criteria Evaluation and Validation Scheme [Internet]. Maryland: National Security Agency [cited 2012 Apr 08]. Available from: http://www.niap-ccevs.org. Examples include National Information Assurance Partnership (NIAP)/Common Criteria Evaluation and Validation Scheme (CCEVS) is "a national program for the evaluation of information technology products for conformance to the International Common Criteria for Information Technology Security Evaluation."

[17] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. "Security control assessments include common controls that are the responsibility of organizational entities other than the information system owner inheriting the controls or hybrid controls where there is shared responsibility among the system owner and designated organizational entities."

From an organizational perspective, security assessments, where there is a shared responsibility[18] conducted by different parts of the same organization, require an appropriate level of independence to ensure the segregation of responsibilities and accountability for maintaining security assessment results.

NOTE

In the FedRAMP Policy Memo, the Office of Management and Budget (OMB) defined four key stakeholders:

- Joint Authorization Board (JAB)—US Department of Defense (DoD), US General Services Administration (GSA), and US Department of Homeland Security (DHS).
- FedRAMP Program Management Office (PMO).
- DHS.
- Federal Agencies.

The FedRAMP PMO described the role of these four stakeholders in the Frequently Asked Question (FAQ) [8]. *"Who are the key organizations involved in FedRAMP?"* In addition, several other roles described in the FAQ were indentified as having a direct and indirect responsibility within FedRAMP. The other roles include:

- National Institute of Standards and Technology (NIST).
- Federal CIO Council.
- Third Party Assessor Organizations (3PAO).
- Cloud Service Providers (CSPs).

The JAB approves the accreditation criteria for third-party assessment organizations (3PAOs) to provide independent assessments of CSPs' implementation of the FedRAMP security authorization requirements [6]. NIST, which has been given responsibilities under FISMA,[19] is responsible for developing the standards and guidelines used within FedRAMP. NIST also plays a supplementary support function indirectly supporting FedRAMP through the establishment of training frameworks[20] and education programs.[21] The FedRAMP PMO coordinated and collaborated with the NIST to develop and implement a formal conformity assessment program[22] to accredit 3PAOs to provide independent assessments of how CSPs implement the FedRAMP requirements [7].

[18] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. Assessments of common controls that are managed by the organization and support multiple information systems.

[19] FISMA was discussed in detail in Chapter 5, Applying the Risk Management Framework.

[20] NIST in leading the National Initiative for Cybersecurity Education (NICE) developed a unified framework for the cybersecurity workforce. Available from: http://csrc.nist.gov/nice/framework/.

[21] From Applying the Risk Management Framework to Federal Information Systems Training [Internet]. Maryland: National Institute of Standards and Technology [cited 2012 April 10]. Available from: http://csrc.nist.gov/groups/SMA/fisma/rmf-training.htm. *NIST developed a training program designed to "provide people new to risk management with an overview of a methodology for managing organizational risk—the Risk Management Framework (RMF)."*

[22] From VanRoekel, S. *Office of Management and Budget (OMB) Memorandum, Security Authorization of Information System in Cloud Computing Environments*. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011. A conformity assessment program provides the capability of producing consistent independent, third-party assessments of security controls implemented by CSPs.

NOTE

Why is FedRAMP accrediting 3PAOs? [8]

Although there currently is no standard or guidance for choosing a 3PAO, the FedRAMP PMO and NIST have designed a conformity assessment process to ensure the independence of and the management and technical quality of 3PAOs using a standard and consistent security assessment process.

When is a 3PAO required? [8]

CSPs that go through FedRAMP must use a 3PAO to provide an independent verification and validation of the security implementations required by FedRAMP. FedRAMP provisional authorizations must include an assessment by a FedRAMP-accredited 3PAO to ensure a consistent assessment process.

PREPARING FOR THE SECURITY ASSESSMENT

Security assessments can be a challenging, time-consuming, and costly activity if the security assessment customer does not appropriately plan and prepare for the security assessment activities. Even before selecting the security assessment provider, the security assessment customer needs to understand its objectives and the information needed to support decisions regarding the impact associated with using an information system. In addition, security assessments can become even more complex, specifically in multi-level or multi-service provider relationships, where security assessment activities may be distributed between more than one service provider. Thereby more focus is required to be placed on the coordination activities, to ensure sufficient information is made available to the security assessor. This situation may also require either working through requests from the other service providers to participate in a security assessment of all of the security controls or to obtain the security assessment results[23] to be included within the current security assessment to inform the security assessment customer.

From the initiation of the security assessment,[24] both parties' involvement is essential to ensure the preparatory (*pre-assessment*) activities conclude with an executable plan for the assessment. As illustrated in Figure 10.1, the security assessment process requires the participation from both the assessment customer and the security assessment provider. During the security assessment,[25] the security

[23] Depending on the length of time between the last assessment and the current assessment, inheritance of assessment results could require additional time to ensure the assessment results are still validate by validating the completeness, accuracy and reliability.

[24] Process for determining how effectively an object of the assessment meets identified security objectives.

[25] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Security control assessments are not about checklists, simple pass-fail results, or generating paperwork to pass inspections or audits-rather, security controls assessments are the principle vehicle used to verify that the implementers and operators of the information system are meeting their state security goals and objectives."*

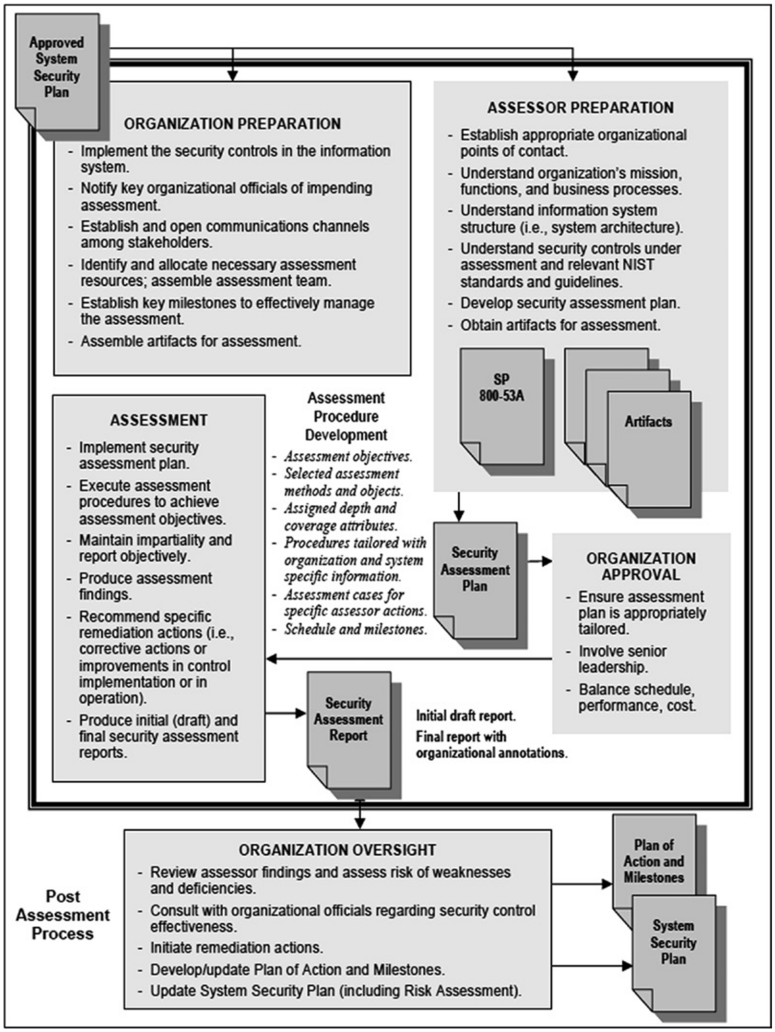

Approved System Security Plan
ORGANIZATION PREPARATION
- Implement the security controls in the information system.
- Notify key organizational officials of impending assessment.
- Establish and open communications channels among stakeholders.
- Identify and allocate necessary assessment resources; assemble assessment team.
- Establish key milestones to effectively manage the assessment.
- Assemble artifacts for assessment.
ASSESSOR PREPARATION
- Establish appropriate organizational points of contact.
- Understand organization's mission, functions, and business processes.
- Understand information system structure (i.e., system architecture).
- Understand security controls under assessment and relevant NIST standards and guidelines.
- Develop security assessment plan.
- Obtain artifacts for assessment.
SP 800-53A
Artifacts
ASSESSMENT
- Implement security assessment plan.
- Execute assessment procedures to achieve assessment objectives.
- Maintain impartiality and report objectively.
- Produce assessment findings.
- Recommend specific remediation actions (i.e., corrective actions or improvements in control implementation or in operation).
- Produce initial (draft) and final security assessment reports.
Assessment Procedure Development
- Assessment objectives.
- Selected assessment methods and objects.
- Assigned depth and coverage attributes.
- Procedures tailored with organization and system specific information.
- Assessment cases for specific assessor actions.
- Schedule and milestones.
Security Assessment Plan
ORGANIZATION APPROVAL
- Ensure assessment plan is appropriately tailored.
- Involve senior leadership.
- Balance schedule, performance, cost.
Security Assessment Report
Initial draft report.
Final report with organizational annotations.
Post Assessment Process
ORGANIZATION OVERSIGHT
- Review assessor findings and assess risk of weaknesses and deficiencies.
- Consult with organizational officials regarding security control effectiveness.
- Initiate remediation actions.
- Develop/update Plan of Action and Milestones.
- Update System Security Plan (including Risk Assessment).
Plan of Action and Milestones
System Security Plan

FIGURE 10.1 Security Controls Assessment Overview [1]

assessment team will rely heavily on the participation and knowledge of the security assessment customer to ensure there is an impartial and objective report of the security control effectiveness, and also a quality assessment, which provides key information needed for decision-makers. This information includes details about the deficiencies and weaknesses that, if compromised (i.e., security controls designed to assure the level of confidentiality, integrity, and availability), could impact mission and business functions supported through the use of the information system. After the security assessment (*post-assessment*), the SAR is generated to build an assurance case.[26] The SAR provides a summary of the security-related information needed for establishing a credible, risk-based decision.

Security Assessment Customer Responsibilities

The customer of the security assessment plays an essential role in the proper planning of the security assessment activities. The security assessment customer is responsible for implementing the security controls, but also has the responsibility of appropriately selecting a qualified security assessment provider, and in determining the objective and scope of the security assessment. In parallel with the preparation activities, the security assessment customer should, at minimum, conduct its own security readiness review. [27] The security readiness review ensures the appropriate security-related information has been organized in a manner that can easily be evaluated by the security assessor. The security assessor uses the security-related information to gain an understanding of the organization's mission and business functions, how those functions are supported by the information system, and how the security controls have been implemented to meet the minimum assurance requirements. The information provided by the security assessment customer should also include a description of any security controls that have not been fully implemented or are planned to ensure the necessary scope is clearly understood for developing an effective security assessment plan (SAP).[28]

Selecting a Security Assessment Provider

The security assessment customer must use its "best judgment" when selecting a security assessment provider to ensure there is an adequate level of independence or there is no conflict of interest, and the security assessment provider has the necessary technical expertise (i.e., knowledge,[29] skills,[30] and abilities[31]).

[26] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"An assurance case is a body of evidence organized into an argument demonstrating that some claim about an information system holds (i.e. is assured)."*

[27] Appendix F of NIST Interagency Report (IR) 7328, *Security Assessment Provider Requirements and Customer Responsibilities*, provides a sample "Customer Readiness Review Checklist."

[28] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The security assessment plan provides the objectives for the security control assessment."*

[29] From Dodaro, G. Federal Information Systems Control Audit Manual: Volume I—Financial Statement Audits. Washington: US Government Accountability Office; 1999. *"Organized body of information, facts, principles, or procedures."*

[30] From Dodaro, G. Federal Information Systems Control Audit Manual: Volume I—Financial Statement Audits. Washington: US Government Accountability Office; 1999. *"Demonstrable and implies a degree of proficiency."*

[31] From Metheny, M. FedRAMP 3PAO Program—Have We Heard of This Idea Before? [Internet]. Florida: International Information Systems Security Certification Consortium (ISC)2 Blog [cited 2012 Apr 22]. Available from: http://blog.isc2.org/isc2_blog/2012/04/fedramp-3pao-program-have-we-heard-of-this-idea-before.html. *"An ability is the power to perform a job function while applying or using the essential knowledge."*

The independence[32] is critical when multiple organizations are responsible for the security control implementations. Therefore, the security assessment customer should determine the most appropriate approach to ensure there is a necessary separation[33] between the security assessment provider and those involved in the development, operations, and management of the information system. This is specifically important when the security assessment customer used a different security assessment provider to develop evidence that will be reused in the current security assessment, or uses the same provider for other security-related services such as implementing remediations/mitigations. In these situations, having the security assessment results reviewed by an independent expert could assist in verifying they are accurate and complete to ensure they are still valid as an objective determination of the state of the security control implementation and effectiveness.

TIP

The FedRAMP 3PAO[34] program was established to accredit organizations based on establishing their ability to meet the requirements of ISO/IEC 17020:1998[35] and to demonstrate the technical competence[36] necessary for conducting security assessment of cloud services. The goal of the conformity assessment[37] process is to ensure the qualified 3PAO:

- Uses a methodology that is aligned with the NIST standards and processes for ensuring cloud services meet the federal government's minimum security requirements.
- Applies a consistent and standardized process for conducting security assessments.

[32] FISMA requires audits to be performed annually through an independent evaluation.

[33] From Government Auditing Standards [Internet]. Washington: US Government Accountability Office [cited 2012 Apr 12]. Available from: http://www.gao.gov/govaud/govaudhtml/index.html. *"Audit organizations that provide nonaudit services must evaluate whether providing the services creates an independence impairment either in fact or appearance with respect to entities they audit."*

[34] From Federal Risk and Authorization Management Program (FedRAMP) [Internet]. Washington: US General Services Administration [cited 2012 Apr 16]. Available from: http://www.gsa.gov/portal/content/118887#9. *"Third Party Assessment Organizations (3PAOs) perform initial and ongoing independent verification and validation of the security controls deployed within the Cloud Service Provider's information system."*

[35] General criteria for the operation of various types of bodies performing inspections—superseded by ISO/IEC 17020:2012.

[36] From Metheny, M. FedRAMP 3PAO Program—Have We Heard of This Idea Before? [Internet]. Florida: International Information Systems Security Certification Consortium (ISC)2 Blog [cited 2012 Apr 22]. Available from: http://blog.isc2.org/isc2_blog/2012/04/fedramp-3pao-program-have-we-heard-of-this-idea-before.html. *"An assessor requires more than pure security knowledge, but also a supplemental knowledge of cloud computing."*

[37] From FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. *"A methodology to demonstrate capability in meeting requirements relating to a product, process, system, person or body as defined by ISO/IEC 17020."*

Security Assessment Planning

The security assessment customer also plays a central role in ensuring the security assessment is conducted effectively and efficiently. In its role, the security assessment customer must ensure that it is not only ready for the security assessment by performing its own readiness review, but it also needs to provide the necessary information (e.g., evidence of prior assessments and artifacts describing security control implementation) and make the resources (e.g., information system access and knowledgeable personnel) available to support the security assessment. The security-relevant information helps security assessors understand the scope of the information system and the security controls being assessed. The more complete and accurate the information, the more tailored the security assessor can make the SAP and supporting assessment procedures. Therefore, prior to the security assessment, the security assessment customer should identify the scope of the assessment and the system components that will be the target of the security assessment. For example, scoping the security assessment could include identifying the number and types of components (i.e., a homogeneous environment which has been consistently configured generally may require less depth or coverage) and determining resource requirements (i.e., accessibility/complexity of the operating environment and use of automated tools versus manual evaluation or inspections techniques).

After the scoping has been completed, the security assessment customer should focus on gathering the security-relevant information for the security assessment provider to evaluate so that a realistic schedule can be developed for conducting the security assessment. Security-relevant information gathered and provided during the security assessment planning can include the following types of information:

- Organizational and system-specific security policies and procedures.
- Descriptions of security control implementation and roles and responsibilities for security controls (e.g., system security plan, standard operating procedures, system diagrams, design documents service level agreements, interconnection agreements, contracts, accreditation packages for common controls, etc.).
- Documents that were developed in support of security control implementation (e.g., contingency plan, risk assessments, incident response plans, plan of action, and milestones, etc.).
- Any extracts from the information system (e.g., audit logs, configuration settings, firewall and intrusion detection/prevention rulesets,[38] evidence generated from previous security assessments, etc.).
- Inventories and hardware/software specifications.

[38] From Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. NIST Special Publication (SP) 800-115, Technical Guide to Information Security Testing and Assessment. Maryland: National Institute of Standards and Technology; 2008. *"A ruleset is a collection of rules or signatures that network traffic or system activity is compared against to determine what action to take."*

TIP

The Cloud Security Alliance (CSA) CloudAudit[39] is a tool that can be used by security assessment customers and leveraged to automate the collection of information (i.e., assertions and artifacts) needed to support a security assessment.

During the security assessment, the security assessor may require assistance from security assessment customer personnel who may have knowledge about how security controls are managed or were integrated into the information system and the operational environment. The security assessment customer should make available key personnel who would need to be interviewed or participate (i.e., conducting security testing) in the security assessment. Depending on the scope of the assessment, coordination and collaboration may be required to limit impacts on the security assessment customer's ongoing operations or existing customers that rely on the services provided by the target information system. Therefore, participation by the security assessment customer is essential to ensure security assessment activities being performed in support of the security assessment are aligned with the agreed-to schedule and milestones.

Security Assessment Provider Responsibilities

The security assessment provider should have a management structure that can deliver a quality security assessment and the technical capabilities to effectively execute the given security assessment. The results of the security assessment execution should provide key decision-makers within the security assessment customer organization (or organizational official(s) that are responsible for making the authorization decision) with the needed security-related information (and supporting evidence) to make a credible, risk-based decision. These security assessment results are compiled by the security assessment provider through the execution of a variety of methods[40] and techniques and supported by the management structure[41] and operational/management systems to ensure the consistency and reliability of the security assessment process, and the quality, accuracy, and completeness of the security-related information.

[39] From CoudAudit [Internet]. Washington, DC: Cloud Security Alliance [cited 2012 August 26]. Available from: https://cloudsecurityalliance.org/research/cloudaudit. "*The goal of CloudAudit is to provide a common interface and namespace that allows enterprises who are interested in streamlining their audit processes (cloud or otherwise)*."

[40] Assessment methods include testing (exercising an assessment object to compare results—expected vs. actual), examining (process used to facilitate understanding how a security control is implemented by examining an assessment object), and interviewing (process used to facilitate understanding how a security control is implemented by conducting interview with organizational personnel).

[41] A framework for managing, planning, and assuring the quality of the assessment.

NOTE

FedRAMP 3PAOs must maintain a management system and technical competence and capability to ensure assessment of cloud services are performed consistently and in compliance with the FedRAMP requirements. The FedRAMP management and technical requirements are summarized as follows:

Management Requirements [2]:

- Conducting inspections and maintain a quality management system in accordance with ISO/IEC 17020.
- Ensuring security assessment team members are competent in performing security assessments.
- Ensuring the protection of proprietary information received as part of the assessment.

Technical Requirements [2]:

- Maintaining knowledge, understanding, and competency in the application of the FedRAMP program security assessment standards, guidelines, and requirements and cloud-based information system-related technologies and practices.
- Maintaining knowledge and understanding in the use of NIST publications and programs.
- Selecting personnel that collectively have the relevant knowledge, skills, and abilities for conducting a security assessment on a given cloud-based information system.
- Preparing an SAP consistent with the FedRAMP requirement, including reviewing the SAP with the cloud service provider.
- Conducting a security assessment with the SAP and preparing a SAR consistent with the FedRAMP requirements.

The requirements established by the FedRAMP PMO ensure the resulting security assessment results and supporting evidence can be leveraged by multiple federal agencies through a single FedRAMP security authorization package.

Selection of Security Assessment Team Members

Similar to the security assessment customer role of selecting a security assessment provider, the security assessment provider has an obligation of conducting due diligence when selecting team members that have the knowledge and expertise in conducting an assessment of the target information system, including experience with the technologies, and also familiarity with the applicable governing federal information security laws, directives, policies, standards, and guidelines.

Developing the Security Assessment Plan (SAP)

The SAP provides the roadmap for executing the security assessment. In the SAP, the rules[42] by which the security assessment provider conducts the security assessment are documented to ensure the security assessment customer understands and agrees

[42] From Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. NIST Special Publication (SP) 800-115, Technical Guide to Information Security Testing and Assessment. Maryland: National Institute of Standards and Technology; 2008. *"Detailed guidelines and constraints regarding the execution of information security testing."*

to the scope of the assessment and also the types of activities that will be performed. The SAP could also include any applicable assumptions and legal considerations (i.e., limitations of liability or non-disclosures to protect both the security assessment customer should any significant issues that occur during or after the assessment). Although the primary responsibility for the development of the SAP is usually the security assessment provider, it should be developed in collaboration with the security assessment customer to ensure the following key points are covered:

- *Scope*—number of components and locations, the types of assessment (or objective), and the depth/coverage.
- *Authorizations*—networks and systems identified by IP address or range and hostname.
- *Logistics*—resource requirements, availability of the location and environment, and testing tools.
- *Data handling*—storage and physical/logical safeguards for data stored at-rest and during transmission, and destruction/sanitization of data after the assessment.
- *Incident response*—definition of the incident and actions that should be taken or guidelines that should be followed by all parties.

The development of the SAP also requires completing several steps to address the key points are covered either within the SAP directly or referenced externally in other contractual documents (e.g., authorization memorandum, engagement or arrangement letter, service agreement, rules of engagement (ROE), service contracts, etc.).

Identify In-Scope Security Controls

The security assessor in the development the SAP must first consider the type of assessment, complete or partial, and the security controls described in the system security plan (SSP), in-place or planned, for meeting the security assessment customer's security requirements. A *complete assessment* is usually performed during the initial authorization or where significant changes have occurred and the scope of the changes cannot be isolated to a specific set of controls and therefore all security controls will be in-scope for the security assessment. A *partial assessment* only focuses on a subset of security controls. The subset of security controls can be those selected as part of the continuous (or ongoing) monitoring activities, security testing performed as part of the normal SDLC which includes assessing a specific set of security controls implemented within the change control process (assuming the scope of the change can be bounded), or where previous assessment occurred and were leveraged, but additional security controls were included to supplement the security control baseline to address unique organizational security requirements. After the purpose of the security assessment has been determined, the SSP and the Continuous Monitoring Strategy[43] are reviewed to select the security controls that

[43] Continuous Monitoring is discussed in detailed in Chapter 11, Strategies for Continuous Monitoring.

would be considered in-scope for the assessment and be used for the remainder of the steps in the SAP development.

Select Assessment Procedures

The security controls identified in the previous step are used by the security assessment provider in selecting the initial set of security assessment procedures.[44] Assessment procedures provide a framework for building assurance cases by demonstrating the effectiveness of security controls implemented within the current operating environment. For each security control selected in the SSP, a complementary assessment procedure is selected. For example, Table 10.1 provides the assessment procedure for CA-2 (*Security Assessment*).

Assessment procedures include one or more objectives for the assessment. The assessment objectives consist of a series of determination statements,[45] which map to the functionality of the security control and assist the security assessor in demonstrating the extent to which a security control is implemented correctly, operates as intended, and produces the desired outcome. In addition, within each assessment objective, methods and objects are used by the security assessment provider during the security assessment. The assessment methods [46] and objects [47] together define the specific actions taken and items selected by the security assessor to produce a finding (or determination of effectiveness) for the security assessment. In Table 10.1, the assessment method for the CA-2.2 assessment objective contains two different types of assessment methods, *examine* and *interview*. The security assessor can use one or both methods to make a determination if the assessment objective is achieved. For the examination assessment method, the security assessor can choose from the identified assessment objects (or other objects not included on the list) to produce the necessary information for the assessor to make a determination of the assessment objective.

[44] NIST Special Publication (SP) 800-53A Revision 1, Appendix F contains a catalog of assessment procedures which are used as a starting point for further tailoring and supplementation.

[45] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The determination statements are linked to the content of the security control (i.e. the security control functionality) to ensure traceability of assessment results back to the fundamental control requirements."*

[46] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Similar to the security control selection process, tailoring and supplementation is applied to the baseline assessment cases."*

[47] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"The item (i.e. specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment."*

Table 10.1 Example Assessment Procedure

CA-2	**SECURITY ASSESSMENT**
CA-2.1	Assessment Objective: *Determine if:*
	(i) *the organization develops a security assessment plan for the information system; and* ***(ii)*** *the security assessment plan describes the scope of the assessment including:*
	– *security controls and control enhancements under assessment;* – *assessment procedures to be used to determine security control effectiveness; and* – *assessment environment, assessment team, and assessment roles and responsibilities*.
	Potential Assessment Methods and Objects: *Examine*: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessments; security assessment plan; other relevant documents or records]
CA-2.2	Assessment Objective: *Determine if:*
	(i) *the organization defines the frequency of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;* ***(ii)*** *the organization assesses the security controls in the information system at the organization-defined frequency;* ***(iii)*** *the organization produces a security assessment report that documents the results of the security control assessment; and* ***(iv)*** *the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative*
	Potential Assessment Methods and Objects: *Examine*: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; other relevant documents or records] *Interview:* [*SELECT FROM:* Organizational personnel with security assessment responsibilities].

TIP

Assessment procedures can form the basis for developing assessment cases.[48] Assessment cases provide a tool for security assessment customers (e.g., federal agency, CSP, communities of interest, etc.) by providing a specific set of assessor actions. The assessment cases represent the specific viewpoint of the community that developed them and present the necessary actions that should be taken to cost-effectively conduct the security assessment. Similar to the security control selection process,[49] tailoring and supplementation is applied to the baseline assessment cases.

Tailor Assessment Procedures

Assessment tailoring involves customizing the assessment procedure to more closely reflect the characteristics of the information system and the operating environment. Customization may be conducted at the organizational level, information system level, or both. The goal of tailoring assessment procedures is to produce the most accurate representation of the security assessment actions necessary to make a determination in the most cost-effective manner. Some assessment procedures may require more tailoring than others or, depending on the phase of the SDLC in which the security assessment is being performed, the assessment procedures may be tailored to focus on a specific aspect of the information system. For example, security assessments conducted during the development/acquisition phase can be tailored to focus on testing very specific functionality to identify deficiencies or weaknesses that may be more costly to remediate in later phases of the SDLC process.

Tailoring involves applying considerations[50] to help guide the selection of potential activities focused on during the assessment. The security assessment customer may provide guidance to assist the security assessor in determining the level of the assessment tailoring that is appropriate for the given assessment. The level of tailoring could also depend on factors such as the available timing and scope for the security assessment. In this chapter we will only focus on two of the tailoring considerations:

- Selecting assessment methods and objects.
- Selecting depth and coverage attributes.

[48] NIST Special Publication (SP) 800-53A Revision 1, Appendix H contains more information on Assessment Cases.

[49] NIST RMF Step 2 (Security Control Selection) was discussed in detail in Chapter 5, Applying the Risk Management Framework.

[50] NIST Special Publication (SP) 800-53A Revision 1, Section 3.2.3 contains a list of consideration for tailoring assessment procedures that could include (1) selecting assessment method and object, (2) selecting depth and coverage attribute values, (3) identifying common controls, (4) developing information system/platform-specific and organization-specific assessments, (5) incorporating assessment results from previous assessments, and (6) obtaining evidence from external providers.

Selecting Assessment Methods and Objects. Security assessors have various options available when selecting assessment methods and objects. Each assessment procedure provides potential options. However, assessors are not necessarily limited to those included in the baseline assessment procedures to obtain the evidence needed to support the determination of security control effectiveness. The actions performed by the security assessors and the types of objects selected for the assessment can be obtained by reviewing the information provided by the security assessment customer as part of the preparatory activities. For example, the SSP and supporting artifacts provided to the security assessors could provide valuable insight into how a particular security control was implemented and what types of methods (e.g., examine, interview, and test) and objects (e.g., specifications, mechanisms, activities, and individuals) would be required for producing evidence and a determination of security control effectiveness.

Selecting Depth and Coverage Attributes. Security assessors also have options for defining the depth and coverage of assessment procedures. The depth and coverage attributes[51] represent the rigor and scope of the assessment and impact the level of effort required for conducting the security assessment. The more detailed the assessment activities, the more resource intensive and time-consuming. However, the more detailed the security assessment, the greater the level of assurance that a particular security control implemented within the information system meets the required security objectives. Although not specifically identifiable[52] in assessment procedures like the methods and objects, the depth and coverage become important factors when building the assurance case during the security assessment execution.

Supplementing Assessment Procedures

The security assessment provider may need to supplement the assessment procedures where security controls unique to an organization or information system do not exist in the baseline security controls (or the assessment procedures do not exist). This could occur where the organization has supplemented the baseline security controls to adequately mitigate organizational-specific risks. In this situation, the additional security controls documented in the SSP would require the security assessor in collaboration with the security assessment customer to develop new assessment procedures.

[51] Basic, focused, and comprehensive.

[52] NIST Special Publication (SP) 800-53A Revision 1, Appendix D contains detailed information on the depth and coverage. In addition, examples of how depth and coverage are applied are shown in the "Potential Assessors Evidence Gathering Actions" in NIST Special Publication (SP) 800-53A Revision 1, Appendix H.

Optimize Assessment Procedures

Optimizing security assessments involves the consolidation or sequencing of assessment procedures to reduce the cost of an associated security assessment. In this activity, the security assessor organizes the assessment procedures in the most efficient way that would enable executing assessment methods and selecting the assessment objects in a manner most likely to produce the desired evidence. For example, some assessment procedures may focus on different aspects of the same control, or different security controls may be integrated into the same components or be related. Therefore, sequencing assessment procedures may facilitate efficiency and reuse of security assessment results.

Finalize and Approve Assessment Plan

Once the SAP has been completed and the assessment procedures have been selected, tailored, and optimized, the security assessment provider must obtain approval from the security assessment customer. This approval acknowledges acceptance and gives the security assessor permission to begin executing the SAP in accordance with the schedule and milestones.

EXECUTING THE SECURITY ASSESSMENT PLAN

The formal approval of the SAP gives the security assessment provider the authorization to begin conducting the security assessment. The SAP utilizes a variety of methods, techniques, and tools during the course of executing the assessment procedures. The assessment procedure provides the necessary information for determining the depth and scope, and will enable the security assessor to select the appropriate testing methodology for the particular type of security assessment. For example, where the security assessment requires conducting penetration testing,[53] the security assessor usually focuses on a scoped and controlled set of components that attempt to identify an attacker (or class of attackers). Since the attackers must operate under constraints, the characterization of the attacker and the tools and techniques[54] will be very specialized to the assessment procedure being executed.

[53] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system."*

[54] The Penetration Testing Execution Standard (PTES) Technical Guidelines is an example resource that assists in developing procedures when conducting penetration testing. Available from: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines.

TIP

The FedRAMP Security Controls Baseline for Moderate-Impact cloud services requires the CSP in CA-7 *(Continuous Monitoring)* to plan, schedule, and conduct assessments annually that include unannounced penetration testing and in-depth monitoring to ensure compliance with all vulnerability mitigation plans [3]. In addition, in RA-5 *(Vulnerability Scanning)*, the CSP is required to employ an independent penetration agent or penetration team to conduct a vulnerability analysis, perform penetration testing based on the analysis of the vulnerabilities to determine their exploitability [3].

The assessment procedures for CA and RA will likely evaluate compliance of the CSP by examining the risk assessment and security assessment policies and procedure, the continuous monitoring plan, vulnerability scan results, and records of vulnerability mitigations and penetration to determine if the CSP, given the existing vulnerabilities within the cloud service, conducted penetration testing (where applicable). The security assessor could conduct formal interviews with CSP personnel that would have the role and responsibility for coordinating and supporting penetration testing, and ensuring the testing was conducted in accordance with the vulnerability mitigation procedures.

During the security assessment, results are produced and documented through actions associated with each assessment objective where selected methods and objects were applied. The security assessment results establish a conclusion about the determination of whether the objectives for the security control have been achieved. The evidence to support the determination is collected and a summary is documented by the security assessor that provides the basis for the finding. Since the findings are meant to be unbiased and objective, the security assessor must present in detail the rationale for why a particular assessment objective was documented as either satisfied (S) or other than satisfied (O).[55] The rationale for establishing an "O" finding may be due to issues other than the security control ineffectiveness. The other issues could include the inability of the security assessor to make a determination where information was insufficient or the unavailability of a particular information system component under examination that was needed for making the determination.

For the security assessment results produced, the security assessment customer should review the findings with specific emphasis on those determinations which result in an "O" finding to determine the significance and to assist in prioritizing findings when developing corrective actions based on the recommendation provided by the security assessor. In addition, the review of the findings may also give an indication there was a lack of understanding by the security assessor of how the

[55] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"For each finding of other than satisfied, assessors indicate which parts of the security control are affected by the finding (i.e. aspects of the control that were deemed not satisfied or were not able to be assessed) and describe how the control differs from the planned or expected state."*

security controls were implemented in the SSP and the security assessment customer may need to provide further clarification to ensure the most accurate reflection of the effectiveness of the security controls is documented in the SAR.

SUMMARY

This chapter provided an introduction to the application of the NIST RMF security assessment process. A three-step framework was presented that covered governing the assessment, preparing for the assessment, and executing the assessment. Additionally, the roles and responsibilities for the security assessment provider and security assessment customer were discussed as they relate to the assessment framework. Finally, the assessment process was covered to address specific factors at each stage of the assessment, to include planning the assessment, executing the assessment, and reporting the security assessment results.

References

[1] Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53A Revision 1, Guide for assessing the security controls in federal information systems and organizations. Maryland: National Institute of Standards and Technology; 2010.

[2] FedRAMP 3PAO Application [Internet]. Washington: US General Services Administration [cited April 11, 2012]. <http://www.gsa.gov/graphics/staffoffices/FedRAMP_3PAO_Application_Materials_010412_Final.zip>.

[3] FedRAMP Security Controls [Internet]. Washington: US General Services Administration [cited April 14, 2012]. <http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip>.

[4] Scarfone K, Souppaya M, Cody A, Orebaugh A. NIST Special Publication (SP) 800-115, Technical Guide to Information Security Testing and Assessment. Maryland: National Institute of Standards and Technology; 2008.

[5] Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2010.

[6] VanRoekel S. Office of Management and Budget (OMB) Memorandum, Security Authorization of Information System in Cloud Computing Environments. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011.

[7] VanRoekel S. Office of Management and Budget (OMB) Memorandum, Security Authorization of Information System in Cloud Computing Environments. Washington, DC: Executive Office of the President, Office of Management and Budget; 2011.

[8] FedRAMP Frequently Asked Questions (FAQs) [Internet]. Washington: US General Services Administration [cited 2012 August 28]. Available from: http://www.gsa.gov/portal/category/102439.

CHAPTER

Strategies for Continuous Monitoring

11

INFORMATION IN THIS CHAPTER:

- Introduction to Continuous Monitoring
- The Continuous Monitoring Process
- Continuous Monitoring within FedRAMP

INTRODUCTION TO CONTINUOUS MONITORING

Continuous[1] monitoring (CM)[2] is an organizational-wide activity that supports risk management by enabling an organization to understand and maintain its information security and risk posture through the collection, analysis, monitoring, and reporting of security-related information. To be effective, CM needs to be driven by the organization's management to ensure it is managed as a part of the enterprise-wide risk management activity. This ensures monitoring is considered outside the context of a single information system, but rather as an integrated part of the organization's risk management function. CM begins by defining the CM strategy. The CM strategy links to the organizational strategies, goals, and objectives, and ensures there is a common understanding of organizational-wide risk tolerance. The risk tolerance is used when determining how to develop and execute a CM program that includes

[1] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information."*

[2] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Information security monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerability, and threats to support organization risk management decisions."*

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00011-3

tasks[3] such as *collecting and reporting on metrics*, *conducting and reporting security control assessments*, *planning, controlling, and maintaining change management and configuration control*, *conducting risk assessments and prioritizing risk responses*.

NOTE

CM is not necessarily a new requirement for the federal government. Historically, as far back as 1995, the National Institute of Standards and Technology (NIST) introduced the concept, as one of two activities[4] used to support operational assurance.[5] At that time monitoring was simply defined as an "ongoing activity that checks on the system, its users, or the environment" [1]. In Office of Management and Budget (OMB) Circular A-130, Appendix III,[6] a government-wide policy was established for federal agencies to review security controls on an ongoing basis through the use of technical tools and techniques.[7] The Federal Information Security Management Act (FISMA) codified CM, by requiring federal agencies to monitor, test, and evaluate information security controls. However, it was not until the publication of the first revision of NIST SP 800-37 that the federal agencies had a systematic model for applying CM within the context of the System Development Lifecycle (SDLC). The NIST security certification and accreditation (C&A) process introduced CM in the forth phase.[8]

The broader CM activity within an organization is implemented through the execution of three major foundational elements:

- Organizational governance.
- CM strategy.
- CM program.

These elements operate together to ensure CM is conducted as an organizational-wide activity that includes the participation from both those responsible for defining the strategy for the organization and those responsible for the day-to-day management of information systems. A common CM approach across the organization enables each level of the organization to more effectively communicate and share

[3] Note, this is not a complete list of activities that can be included within an organization's continuous monitoring program needed to maintain a situational awareness of the information system and operating environment.

[4] The difference between system audits and monitoring focused on the notion of "real time."

[5] From Guttman, B., Rockback, E. NIST Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook. Maryland: National Institute of Standards and Technology; 1995. *"Operational assurance is the process of reviewing an operational system to see that the security controls, both automated and manual, are functioning correctly and effectively."*

[6] *Office of Management and Budget (OMB) Circular A-130, Appendix III*. Available from: www.whitehouse.gov/omb/circulars_a130_a130appendix_iii.

[7] From Office of Management and Budget (OMB). OMB Memorandum Circular A-130, Appendix III, Security of Federal Automated Information Resources. Washington: Executive Office of the President, Office of Management and Budget; 2000. *Example included virus scanners, vulnerability assessment products, and penetration testing.*

[8] The CM program addressed three tasks: *configuration management and control, security control monitoring,* and *status reporting* and *documentation.*

information that would support a cost-efficient, resilient, and timely[9] risk management strategy. The increasing reliance on information technology (IT) for supporting the organization's mission and as a critical part of its business operations requires accurate and up-to-date information for making continuous risk-based decisions. Using a standardized CM approach enables the security- and risk-related information to be produced both cost-effectively and efficiently through a managed set of resources and processes.

Organizational Governance

The management of risk requires a "top-down" approach, led by management, with the establishment of the CM strategy. The CM strategy is implemented through a comprehensive CM program. The role of governance[10] is to ensure the CM strategy is consistently applied through a CM program across the organization. The process for implementing CM, briefly introduced in this section and discussed in detail later in this chapter, requires an effective integration into the organization's governance structure. Governance manages the CM strategy and program through the CM processes, which include:

- Defining a strategy for continuous monitoring;
- Developing and implementing a CM program;
- Analyzing data and reporting findings;
- Responding to findings; and
- Reviewing and updating[11] the ISCM strategy and program [2].

In Figure 11.1, the organization-wide view focuses on illustrating how CM supports the risk-based decisions made at the various levels within an organization. In the three-tiered model, tier 1 focuses on strategic CM activities that support governance[12] decisions based on security-related information from the implementation of CM activities at tiers 2 and 3. The model also represents the alignment that must exist between the CM process and the risk management process, as discussed in

[9] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *Risk management decisions, assessment and responses need to be able to scale with emerging security issues, and any decision-making needs to be based on the most relevant and accurate information.*

[10] Governance models are discussed in detail in Chapter 6, Risk Management.

[11] The CM strategy and program are viewed for relevance and are revised as needed to increase visibility into assets and awareness of vulnerabilities.

[12] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. Maryland: National Institute of Standards and Technology; 2011. *"Governance is the set of responsibilities and practices exercised by those responsible for an organization (e.g. the board of directors and executive management in a corporation, the head of a federal agency) with the express goal of: (i) providing strategic direction; (ii) ensuring that organizational mission and business objectives are achieved; (iii) ascertaining that risks are managed appropriately; and (iv) verifying that the organization's resources are used responsibly."*

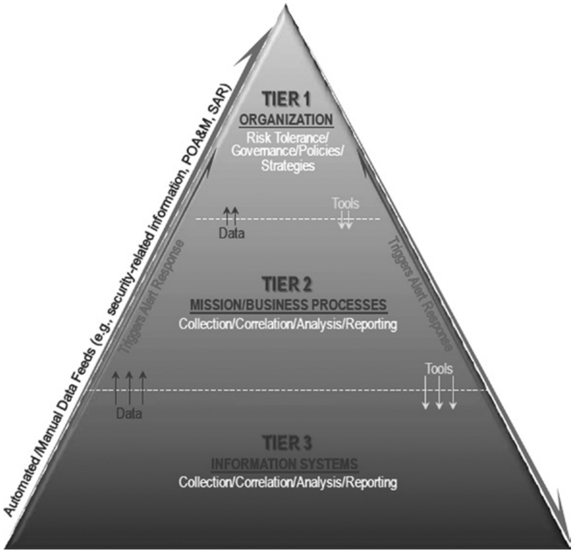

Automated/Manual Data Feeds (e.g., security-related information, POA&M, SAR)
TIER 1
ORGANIZATION
Risk Tolerance/
Governance/Policies/
Strategies
Data
Tools
Triggers Alert Response
Triggers Alert Response
TIER 2
MISSION/BUSINESS PROCESSES
Collection/Correlation/Analysis/Reporting
Data
Tools
TIER 3
INFORMATION SYSTEMS
Collection/Correlation/Analysis/Reporting

FIGURE 11.1 Organization-Wide View of CM [2]

Chapter 6, so that the monitoring strategy produces information that is relevant and useful when making risk-related decisions at each organizational tier. Tier 1 addresses risk management from a strategic perspective by developing a governance policy that drives the CM strategy and communicates the organization's risk management strategy. In tier 2, CM security-related information is dependent on the specific importance of the mission/business processes to the overall organizational goals and objectives. Therefore, it is critical to have an understanding of the security impacts to ensure appropriate implementation of CM activities for information systems that support mission/business processes. In tier 3, CM activities focus on the information system-level security controls to ensure they implement the organization security requirements and continue to be effective over time.

Metrics[13] developed at each tier guide the collection of security-related information used in making risk-based decisions. Therefore, it is important for organizations to select the most appropriate tools and techniques[14] that present information in a format that will be useful for a specific organizational tier. The format also enables the data

[13] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Metrics are designed to present information in a context that is meaningful for each tier."*

[14] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Organization-wide monitoring cannot be efficiently achieved through manual processes alone or through automated processes alone."*

that will be collected,[15] correlated, analyzed, and reported to be effectively communicated to provide stakeholders with the most accurate indication of the security posture.[16] Since metrics are a key part[17] of CM, the organization may need to refine and update[18] the metrics so they "continue to be relevant, meaningful, actionable, and supportive of risk management decisions made by organizational officials at all tiers" [2].

In addition, federal agencies have legislative and regulatory drivers for capturing metrics that enable them to measure[19] the performance of security related to their program goals and objectives. The GPRA Modernization Act[20] requires a quarterly performance assessment of all government programs to assess performance and improvement. The long-term strategic planning[21] described in the GPRA Modernization Act requires federal agencies to define performance goals[22] and objectives, and the performance objectives that are reported on quarterly. Each performance plan includes "a balanced set of performance indicators to be used in measuring or assessing progress toward each performance goal" [3]. FISMA[23] requires federal agencies to report[24] on the status of their information security programs. The annual FISMA

[15] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Data collection primarily occurs at the information systems tier."*

[16] From Federal Network Security Branch. Continuous Monitoring and Risk Scoring (CM/RS) Concept of Operations (CONOPS) for Supporting Agency Cyber Security Operations. Washington: US Department of Homeland Security; 2011. *Security posture is the state of effectiveness to agency implemented security controls.*

[17] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Care must be taken in determining how best to use security-related information from individual information systems in calculating organizational metrics for security and risk."*

[18] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Organizations," security architectures, operational security capabilities, and monitoring processes will improve and mature over time to better respond to the dynamic threat and vulnerability landscape."*

[19] NIST uses "measures" to refer to the results of data collection, analysis, and reporting. Available from: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

[20] The Government Performance Results Act (GPRA) of 1993 was modernized in 2010. Available from: http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m.

[21] From Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., Robinson, W. NIST Special Publication (SP) 800-55 Revision 1, Performance Management. Maryland: National Institute of Standards and Technology; 2011. *"Information security must be explicitly tied to at least one goal or objective in the strategic planning process to demonstrate importance in accomplishing the agency's mission."*

[22] From GPRA Modernization Act of 2010 [Internet]. Washington: US Government Printing Office [cited 2012 April 28]. Available from: http://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf. *Strategic plans include outcome-oriented goals and objectives, and a description of how the goals and objectives are achieved through operational processes, skills and technology, and human capital, etc.*

[23] FISMA is discussed in detail in Chapter 5, Applying the Risk Management Framework.

[24] Status reporting is performed annually and requires federal agencies to summarize the performance of their security programs used to secure all information and information systems.

report summarizes the performance of the federal agency's program to secure all of your agency's information and information systems [4].

CM Strategy

The CM strategy aligns the CM activities with the organization-wide risk management strategy.[25] Through an understanding of the organization's strategic goals and objectives, the CM requirements can be developed to address the monitoring and assessment frequency of security controls, and customize status reporting to ensure consistency across the organization. This further supports each of the organizational tier's information needs required for making risk-based decisions. For the strategy to be effective and support the organization's risk management function, it needs to be comprehensive, broadly encompassing the technology, processes, procedures, operating environment, and people [2].

The organization's information requirements can be different at each of the organizational tiers, requiring strategies tailored specifically to a tier. Therefore, to meet the goal of maintaining consistency across the organization, the implementation of the organization-wide CM strategy needs to be driven by the leadership to ensure the CM strategy evolves as requirements for information change at each tier. In addition to enabling information reuse across the organization, a consistent understanding of the CM strategy ensures a cost-effective implementation of the processes, procedures, tools, and techniques to all organizational information systems, achieving a broad organization-wide situational awareness. The CM strategy can also help the organization use an integrated approach to more efficiently react, such as by changes in a single information system or in the organization's threat environment.

TIP

The CM strategy [2] should:

- Reflect the organization's risk tolerance (including helping set priorities and consistent management of risk);
- Include metrics that provide meaningful indications of security status at all organizational tiers;
- Ensure continued effectiveness of all security controls;
- Address verifying compliance with information security requirements derived from organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines;
- Be informed by all organizational IT assets and aids to maintain visibility into the security of the assets;
- Ensure knowledge and control of changes to organizational systems and environments of operation; and
- Maintain awareness of threats and vulnerabilities.

[25] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"The ISCM strategy is developed and implemented to support risk management in accordance with organizational risk tolerance."*

An organization-wide CM strategy provides a comprehensive view of the CM requirements of all organizational tiers. These requirements may be derived from multiple sources including the key metrics and the frequency of security controls monitoring and assessments deemed necessary to provide an indication of the information security and risk posture. CM strategies can also be developed at a specific tier[26] to

NOTE

In July 2010, OMB released a policy[27] which clarified the roles and responsibilities for cybersecurity. In this policy, the Department of Homeland Security (DHS)[28] was identified as having the responsibility for implementing the operational aspects of the cybersecurity of civilian federal information systems as defined in FISMA under section 3543.[29] The scope of responsibility as it relates to CM included the government-wide and agency-specific monitoring and assessment of areas such cybersecurity operations and incident response [5]. In addition, DHS's role was further clarified in a Federal Information Security Memorandum[30] published in August 2011 in which federal agencies were required to report[31] to DHS on metrics through automated[32] or manual data feeds. For example, in February 2012, DHS[33] identified Administrative Priorities (AP)[34] that would be scored along with Key FISMA Metrics (KFM).[35] Within the AP, CM was identified as a "key element to managing an information security program is having accurate information about security postures, activities and threats" [6].

[26] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"A continuous monitoring strategy for an individual system may also include metrics related to its potential impact on other systems."*

[27] Office of Management and Budget (OMB) Memorandum 10–28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*. Available from: www.whitehouse.gov/omb/assets/memoranda_2010/m10-28.pdf.

[28] From Zients, J., Kundra, V., Schmidt, H. Office of Management and Budget (OMB) Memorandum 10–15, FY 2010 Reporting Instructions for the Federal Information System Management Act and Agency Privacy Management. Washington: Executive Office of the President, Office of Management and Budget; 2010. *DHS will provide additional operational support to federal agencies in securing federal systems.*

[29] FISMA was discussed in detail in Chapter 5, Applying the Risk Management Framework.

[30] From Lew, J. Office of Management and Budget (OMB) Memorandum 11–33, FY 2011 Reporting Instructions for the Federal Information System Management Act and Agency Privacy Management. Washington: Executive Office of the President, Office of Management and Budget; 2011. *"The Department of Homeland Security issues Federal Information Security Memoranda to inform federal departments and agencies of their responsibilities, required actions, and effective dates to achieve federal information security policies."*

[31] From Lew, J. Office of Management and Budget (OMB) Memorandum 11–33, FY 2011 Reporting Instructions for the Federal Information System Management Act and Agency Privacy Management. Washington: Executive Office of the President, Office of Management and Budget; 2011. *The reporting requirements will mature over time as the efforts of the Chief Information Officer (CIO) Council's Continuous Monitoring Working Group (CMWG), in collaboration with the agencies, evolve and additional metrics and capabilities are developed.*

[32] Security automation is discussed in Chapter 6, Cost-Effective Compliance Using Security Automation.

[33] DHS National Cyber Security Division (NCSD), Federal Network Security (FNS).

[34] Areas of continuous monitoring determined to be administrative priorities include: *asset management*, *configuration management*, and *vulnerability management*.

[35] Additional metrics outside of the administrative priorities.

address local requirements. However, to enable an organization-wide approach to CM, tier-specific strategies will need to be driven from a consistent application of the methodologies and practices used at the higher organizational tiers (i.e., tier 3 strategies should encompass tier 2 policies, procedures, and processes). This ensures that any condition that would require the tier-specific strategy to be updated also triggers additional updates to strategies in the higher tiers so that security-related information captured at the lower tiers maintains relevance in supporting organization-wide risk-based decisions across the organization.

CM Program

Although more tactically focused, the organization's CM program facilitates the implementation of the CM strategy. The scope of the program should be designed to address the sufficiency in security-related information to support risk-based decisions. This can be accomplished by defining metrics and frequencies[36] of monitoring and assessment that produce the needed information. The development of a Continuous Monitoring Plan[37] facilitates the implementation of the CM program. The Continuous Monitoring Plan also addresses the integration of CM activities and metrics to support the CM strategy through the identification of security controls necessary for monitoring to ensure their effectiveness[38] over time.

As previously mentioned, metrics provide a guide for collecting security-related information. The types of metrics defined for the organization reflect the security objectives for the organization, mission/business processes, and/or information system. In addition, metrics can be defined at any organizational tier. Therefore, the organization will need to ensure that the frequency of monitoring, if not consistent across the organizational tiers, has a linkage between the security-related information requirements.

THE CONTINUOUS MONITORING PROCESS

For CM to be an effective tool and operate as a source of information for supporting the management of risk, the organization needs to ensure the requirements and activities at each level of the organization are addressed in the CM strategy. This enables

[36] The frequency of monitoring and assessment should be sufficient to meet the organization's security assurance requirements. NIST Special Publication (SP) 800-53, Appendix E, discusses security assurance.

[37] From VanRoekel, S. Security Authorization of Information Systems in Cloud Computing Environments. Washington: Executive Office of the President, Office of Management and Budget; 2011. *"Authorization packages contain the body of evidence needed by authorizing officials to make risk-based decisions regarding the information systems providing cloud services. This includes, as a minimum, the Security Plan, Security Assessment Report, Plan of Action and Milestones and a Continuous Monitoring Plan."*

[38] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"The measure of correctness of implementation (i.e. how consistently the control implementation complies with the security plan) and how well the security plan meets organizational needs in accordance with current risk tolerance."*

risk management activities to more closely reflect the type of security-related information collected as part of the CM program and used for making risk-based decisions. As an example, Figure 11.2 provides a high-level illustration of the alignment that exists between the CM strategy and the organizational tiers. In addition, it also depicts the inputs that can be potential sources for deriving requirements that need to be addressed by the strategy for implementing an organization-wide CM program.

The CM process includes both *strategic* and *programmatic* activities. The strategic activities usually occur at the higher level within the organization where the overall organizational risk tolerance is defined. However, CM strategies can exist at individual tiers to address requirements specific to a mission or business process supported by the information system or information systems where stakeholders exist across more than one business unit or federal agency. To ensure security-related information collected or resources required to support tier-specific requirements are reusable, organizations should make sure there is some consistency with higher-level tiers.

Defining a CM Strategy

The CM strategy reflects the organizational driver for CM within the organization. The execution of the CM program is facilitated through requirements and activities included in the strategy. The requirements and activities are defined in policies, procedures, and templates that support the CM strategy such as metrics,

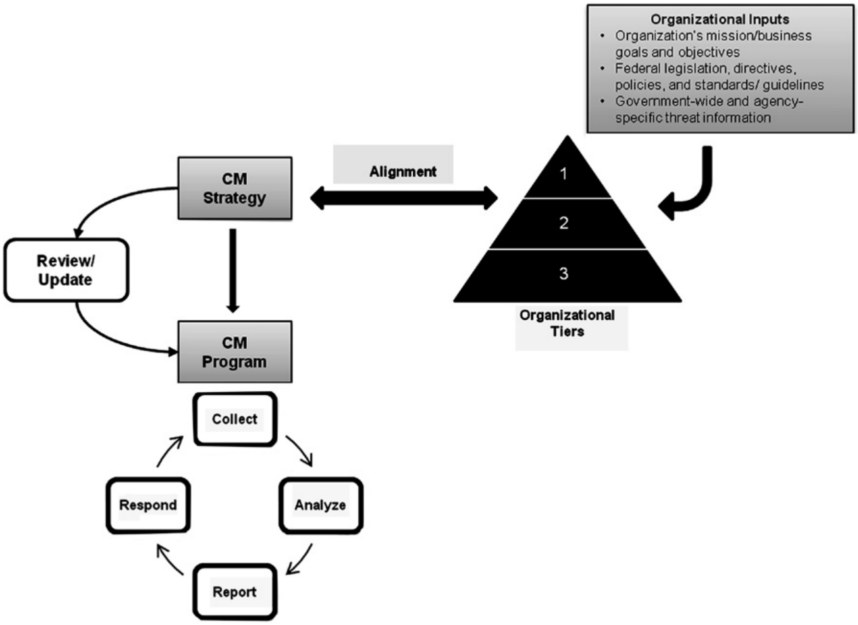

Organizational Inputs
• Organization's mission/business goals and objectives
• Federal legislation, directives, policies, and standards/ guidelines
• Government-wide and agency-specific threat information
CM Strategy
Alignment
1
2
3
Organizational Tiers
Review/ Update
CM Program
Collect
Analyze
Report
Respond

FIGURE 11.2 Integration of CM Process with Organization-Wide Risk Management

review/updates, assessment and status monitoring and reporting, risk assessments, and configuration management. These policies, procedures, and templates are supported through processes that addresses the requirements at the most appropriate level within the organization to ensure risks can be managed at the organizational risk tolerance.

Strategies developed at the information system tier align more closely with the NIST Risk Management Framework (RMF).[39] CM within the NIST RMF will be discussed in more detailed later in this chapter. For the purpose of this section, it is important to understand that security-related information produced through tier 3 strategies and programs supports the organizational CM strategy and program at tiers 1 and 2. Management responsible and accountable for risk-based decisions at tier 1 or 2 are informed with regards to organizational risk based on information produced at the lower tiers so that appropriate mitigation strategies can be developed and implemented. In addition, the tier 3 CM strategy also supports ongoing authorizations [2].

Implementing a CM Program

The CM strategy is implemented through the CM program.[40] The scope of the program should address the requirements[41] defined in the strategy for the security-related information needed by the organization for making risk-based decisions. These requirements can be across all tiers, or specific to a tier, but should include at a minimum [8]:

- Monitoring metrics.
- Frequency of monitoring and assessments.
- Security status reporting.

[39] From Zients, J., Kundra, V., Schmidt, H. Office of Management and Budget (OMB) Memorandum 10–15, FY 2010 Reporting Instructions for the Federal Information System Management Act and Agency Privacy Management. Washington: Executive Office of the President, Office of Management and Budget; 2010. *"Agencies should develop an enterprise-wide strategy for selecting subsets of their security controls to be monitored on an ongoing basis to ensure all controls are assessed during the three-year authorization cycle."*

[40] From Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 4 (Initial Public Draft), Security and Privacy Controls for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2012. *"Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions."*

[41] From Zients, J., Kundra, V., Schmidt, H. Office of Management and Budget (OMB) Memorandum 10–15, FY 2010 Reporting Instructions for the Federal Information System Management Act and Agency Privacy Management. Washington: Executive Office of the President, Office of Management and Budget; 2010. *"A robust and effective continuous monitoring program will ensure important procedures included in an agency's security authorization package (e.g. as described in system security plans, security assessment reports, and [Plans of Actions and Milestones] (POA&Ms)) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security state of the information system on an ongoing basis."*

NOTE

In August 2011, DHS released FISM 11-02, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. DHS was given the authority to provide direction on government-wide metrics and submit information according to the defined reporting activities and frequency. The activities [4] included:

- Data feeds;
- Security question responses;
- Cyberstat accountability sessions/agency interviews.

This government-wide CM strategy was developed through collaboration with the Federal Chief Information Officer (CIO) Council Information Security and Identity Management Committee (ISIMC) Continuous Monitoring Working Group (CMWG). The CMWG focused on the establishment of a government-wide continuous monitoring and risk-scoring capability and the technology, people, and processes used to implement the capability to enhance the overall security posture of the federal government [7].

The metrics defined by the organization can come from any tier across the organization and encompass different sources of security-related information. In addition, the information can be collected either through manual procedures and techniques[42] or automated tools and technologies.[43] The frequency can also vary based on the source of the requirements used as an input to the CM strategy. As an example, in February 2012, US Department of Homeland Security (DHS) published the FISMA metrics[44] that were required by federal agencies to incorporate into their CM program for collection and reporting. Table 11.1 presents the current metrics related to CM.

Metrics used for measuring the organization's security posture may also be determined to be different depending on the organizational tier (see Figure 11.1) where they are defined. For example, tier 1 metrics may be defined by the department/agency CIO and/or Chief Information Security Officer (CISO) based on a CM strategy that focuses on providing an organizational-wide view of the security posture at tiers 2 and 3, and to support security governance decisions. Whereas tier 3 metrics may be defined by the System Owner and/or Information System Security Officers (ISSOs) based on information collected for determining the security posture associated with the security control effectiveness in a specific information system and to support ongoing authorization decisions.

Defining the frequency of monitoring and assessment activities is essential for the implementation of an effective CM program. Establishing the frequency requires understanding the organization objectives for monitoring and assessments.

[42] For manual CM processes to be effective, they must be repeatable.

[43] Automation can ensure process consistency and efficiency.

[44] Metrics to support FISMA reporting may be an aggregate of information that is from various levels and sources from across the organization (i.e., governance, operations, and information system).

For example, the following criteria [2] can assist an organization in determining the frequency:

- Security control volatility.
- System categorization/impact level.
- Security controls or specific assessment objectives providing critical functions.
- Security control with identified weaknesses.
- Organizational risk tolerance.
- Threat/vulnerability information.
- Risk assessment results.
- Output of monitoring strategy reviews.
- Reporting requirements.

Table 11.1 Continuous Monitoring Performance Metrics [9]

Perfomance Areas	Metrics
Asset Management (*Hardware*)	• Total number of organization hardware assets connected to the organization's network • Number of assets where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets • Frequency (in days) at which automated capabilities are conducted on all assets • Time (in days) it takes to complete the device discovery process • Number of assets where identifying information is collected: *network IP address*, *hostname*, and *MAC address* • Number of assets where an automated capability exists to determine whether the asset is authorized and who manages the asset • Number of assets where an automated capability exists to identify and remove (manually or automated techniques such as through network access controls) unauthorized assets • Time (in days) it takes to assign management for the asset (i.e., authorize) or remove (i.e., unauthorize) the asset once identified • Number of assets where automated capabilities exist to detect and mitigate routes (including those across air-gapped networks)
Asset Management (*Software*)	• Number of installed operating systems (i.e., vendor, product, version number, and patch level) • Number of hardware assets where the operating system are installed to assess vulnerabilities without conducting a scan • Number of enterprise-wide commercial-off-the-shelf (COTS) applications installed on assets • Number of hardware assets where an automated capability exists to detect and block unauthorized software from executing

Table 11.1 Continuous Monitoring Performance Metrics (*continued*)

Perfomance Areas	**Metrics**
Configuration Management (*Operating Systems*)	• Number of installed operating systems (i.e., vendor, product, version number, and patch level) where a secure configuration baseline has been defined • Number of hardware assets where installed operating systems (i.e., vendor, product, version number, and patch level) have a secure configuration baseline • Percentage of hardware assets where the operating system software has an automated capability to identify deviations from approved secure configuration baselines and provide visibility to through enterprise-level reporting • Frequency (in days) the automated capability to identify operating system software deviations from approved secure configuration baselines is conducted
Configuration Management (*Applications*)	• Number of enterprise-wide commercial-off-the-shelf (COTS) applications installed on assets where a secure configuration baseline has been defined • Number of hardware assets where installed applications have a secure configuration baseline • Percentage of hardware assets where the application has an automated capability to identify deviations from approved secure configuration baselines and provide visibility to through enterprise-level reporting • Frequency (in days) the automated capability to identify application deviations from approved secure configuration baselines is conducted
Configuration Management (*Configuration Baselines*)	• Number of hardware assets which the FDCC[a]/USGCB[b] baseline application has • Number of FDCC/USGCB baselines (in CCE[c]) where approved deviations exists from the FDCC/USGCB standards • CCE and number of hardware assets where the FDCC/USGCB standard applies but has approved deviations
Vulnerability Management	• Number of hardware assets where an automated capability exists to identify CVEs[d] from the National Vulnerability Database[e] and provide visibility to through enterprise-level reporting • Number of hardware assets identified that are evaluated using tools to assess the security of the systems and generate output compliant with CVE, CVSS[f], and OVAL[g]

[a] *Federal Desktop Core Configuration. Available from: http://nvd.nist.gov/fdcc/index.cfm.*
[b] *United States Government Configuration Baseline. Available from: http://usgcb.nist.gov.*
[c] *Common Configuration Enumeration. Available from: http://cce.mitre.org.*
[d] *Common Vulnerability and Exposure. Available from: http://cve.mitre.org.*
[e] *National Vulnerability Database. Available from: http://nvd.nist.gov.*
[f] *Common Vulnerability and Scoring System. Available from: http://www.first.org/cvss/cvss-guide.*
[g] *Open Vulnerability and Assessment Language. Available from: http://oval.mitre.org.*

NOTE

The US Department of State established the iPost Risk Scoring Program to provide summary and detailed information on the current status of hosts[45] at a particular site.[46] In 2010, DHS released the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture Report.[47] CAESARS was based in part on iPost.[48] DHS indicated that analyzing security-related information, defining and calculating risk, and assigning scores is a key part of the continuous monitoring process [10]. However, it is important to note that some management and operational controls cannot be effectively scored and some aspect of risk management cannot be automated. The Federal CIO Information Security and Identity Management Committee (ISIMC) established an initiative that would extend the DHS CAESARS. The goal of the CAESARS Framework Extension (FE)[49] was to present a technical reference model to allow organizations to aggregate collected data from across a diverse set of security tools, analyze that data, perform scoring, enable user questions, and provide overall situational awareness [11].

The collection and reporting of security-related information is supported by the CM architecture. Security automation[50] facilitates CM through an increase in the coverage and efficiency of information collection. To make the information useful and reusable, consideration should be given to ensure the data supporting the CM strategy and program is interoperable[51] across the organization. Since accountability for the security posture may exist with different roles/functions within or between different organizations, the data needs to be portable when supporting different

[45] Computer connected to a network.

[46] From Williams-Bridgers, J. State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain. Washington: US Government Accountability Office; 2011. *"Sites, or operational units, within iPost are either identified based on physical location, such as an overseas embassy or domestic facility within the United States, or can be grouped by administrative responsibility or function, such as all hosts within a particular bureau."*

[47] NIST extended the CAESARS framework to address enterprise continuous monitoring. Available from: http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7756.

[48] From Department of Homeland Security, Federal Network Security Branch. Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture Report Version 1.8. Washington: US Department of Homeland Security; 2010. *"A target-state reference architecture is proposed for security posture monitoring and risk scoring, based on the work of three leading federal agencies: the Department of State (DOS) Security Risk Scoring System, the Department of Treasury, Internal Revenue Service (IRS) Security Compliance Posture Monitoring and Reporting (SCPMaR) System, and the Department of Justice (DOJ) use of BigFix and the Cyber Security Assessment and Management (CSAM) tool along with related security posture monitoring tools for asset discovery and management of configuration, vulnerabilities, and patches."*

[49] The CAESARS FE builds upon the DHS CAESARS to address requirements that would make it applicable to the US Department of Defense (DoD), Intelligence Community (IC), and the Civilian Agencies.

[50] Security automation is discussed in detail in Chapter 12, Cost-Effective Compliance Using Security Automation.

[51] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Interoperable data specifications (e.g. SCAP, XML) enable data to be collected once and reused many times."*

metrics or different monitoring and assessment frequencies [2]. Although briefly mentioned in this section, the next chapter discusses security automation in more detail as it relates to supporting CM requirements.

The implementation of the CM program involves operationalizing the organizational policies and procedures defined at tiers 2 and 3. The policies and procedures include identifying the types of reports,[52] the recipients of the reports, the frequency of reporting, and any tools and methodologies. In addition, processes and capabilities[53] at tiers 2 and 3 should be designed to enable the effective collection, analysis, reporting, and response. The collection of security-related information can be manual or automated, with emphasis placed on the assembly of the information to ensure it is in a format that makes it meaningful to stakeholders and provides the necessary visibility for making risk-based decisions.

The analysis and reporting of security-related information is conducted at tiers 1 and 2 as an aggregate view of the security status of operational and system-level security controls from across the organization. Tier 3 analysis and reporting primarily supports ongoing authorizations and system-level mitigations. The processes and capabilities support the analysis and reporting by enabling organizations to consistently and efficiently measure security, determine the effectiveness of security controls, and prioritize remediation actions.

A response to findings from CM analysis may require coordination with other stakeholders across the organization. Responses can occur at each organization tier (e.g., tier 1 responses focus on those aspects which mitigate risk[54] through governance and policies and tier 3 responses mitigate risk associated with system-level security policies, procedures, processes, and security controls). Responses could also include changes to the CM strategy and program discussed in the next section.

Review and Update CM Strategy and Program

As previously discussed, the CM strategy and program evolves and must continue to be applicable to the organization's mission/objectives and operation/threat environment. CM is a recursive process in which the monitoring strategy is continually refined [2]. As changes occur to the strategy, the program may need to be reviewed and updated to support the organization's risk tolerance and to ensure the security-related information continues to be relevant and accurate.

[52] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *Examples include reoccurring reports, automated reports, ad hoc reports, data feeds and database views.*

[53] Continuous monitoring capabilities are enabled through technologies and techniques that provide the organization with the most accurate picture of the security and risk posture, visibility into and near or real-time data through manual or automated data feeds.

[54] Risk responses are discussed in detail in Chapter 6, Risk Management.

NOTE

Changes to the CM strategy could occur due to the following factors [2]:

- Mission/business processes,
- Enterprise architecture,
- Organizational risk tolerance,
- Threat/vulnerability information,
- Plan of action and milestones (POA&Ms),
- Security trends,
- Federal laws or regulations,
- Reporting requirements.

The tier 1 and 2 policies and procedures should address the process for reviewing and updating the strategy. The process should consider potential aspects [2] of the strategy that ensure sufficiency of the information to support the organization risk management decisions[55] such as:

- Measurements,
- Metrics,
- Monitoring frequencies, and
- Reporting requirements.

CONTINUOUS MONITORING WITHIN FEDRAMP

The Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO) established a Concept of Operations (CONOPS)[56] that included the framework for CM within FedRAMP.[57] In addition, the FedRAMP PMO published a CM Strategy[58] for use once the Cloud Service Provider (CSP) receives a Provisional Authorization.[59] Although the specific aspects of CM implemented within FedRAMP are primarily limited to tier 3 CM activities, it is important to discuss how the organization-wide CM discussed earlier in this chapter supports the implementation of the FedRAMP CM process. Within the context of FedRAMP, the goal of CM is to enable visibility into the security posture of cloud services to support continuous risk management decisions. This visibility is achieved through reporting from the CSP in three areas: *operational visibility*, *change control*, and *incident response*.

[55] Risk management decisions include: *risk response*, *ongoing authorization*, and *resource/prioritization*.

[56] FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) Version 1.1. Available from: http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

[57] Referred to as ongoing assessment and authorization.

[58] FedRAMP Program Management Office (PMO). Continuous Monitoring Strategy & Guide. Available from: http://www.gsa.gov/graphics/staffoffices/Continuous_Monitoring_Strategy_Guide_072712.pdf.

[59] FedRAMP Program Management Office (PMO). Continuous Monitoring Strategy & Guide, Version 1.1. Washington: US General Services Administration; 2012. *"To receive reauthorization of a FedRAMP Provisional Authorization from year to year, CSPs must monitor their security controls, assess them on a regular basis, and demonstrate that the security posture of their service offering is continuously acceptable."*

Table 11.2 FedRAMP CM Roles and Responsibilities [12]

FedRAMP PMO	CSP	Federal Agency
• Work in coordination with DHS to establish a framework for continuous monitoring, incident response and remediation, and FISMA reporting	• Obtain an independent third-party assessment of required security controls to support ongoing assessments and authorizations • Maintain Continuous Monitoring programs • Comply with Federal Requirements for Change Control and Incident Reporting	• Continuously monitor security controls that are the agency's responsibility

The FedRAMP PMO, CSP, and federal agency each have organizational CM roles and responsibilities when executing CM activities within the context of FedRAMP. Table 11.2 outlines those FedRAMP CM roles and responsibilities.

Each operates as an essential stakeholder that supports the effective integration of organization-wide CM into the FedRAMP process. As illustrated in Figure 11.3, each stakeholder plays a role in the management of risk by ensuring CM is applied consistently across the organizational tiers through common CM policies, procedures, processes, and templates.

In addition, FedRAMP establishes a methodology that enables the federal government to leverage security-related information that can be applied over more than one cloud service, effectively improving government-wide security. However, it is important to note that the CSP's role in CM is not a substitute for the federal government's responsibility and accountability for the use of cloud services.

FedRAMP includes two primary components to CM: *security documents* and *real-time operational feeds*. These components enable ongoing authorization through the recurring updates of key security documents (i.e., system security plan, security assessment report, and POA&Ms) and operational visibility. The real-time operational feeds support CM by reducing the administrative barriers needed to demonstrate compliance by shifting to real-time oversight monitoring [12].

Through the three-tiered approach, the FedRAMP PMO, CSP, and federal agency can ensure the CM strategy and program can be used to maintain the cloud service's authorization to operate. The tasks outlined in Figure 11.4 support the three CM areas within the FedRAMP CM process by ensuring system information is kept up-to-date while also facilitating risk-based decisions on an ongoing basis through the assessment and monitoring of security controls (*common, hybrid,* or *system-level*) using security management and reporting tools.[60] This transforms the

[60] Security automation is discussed in detail in Chapter 12, Cost-Effective Compliance Using Security Automation.

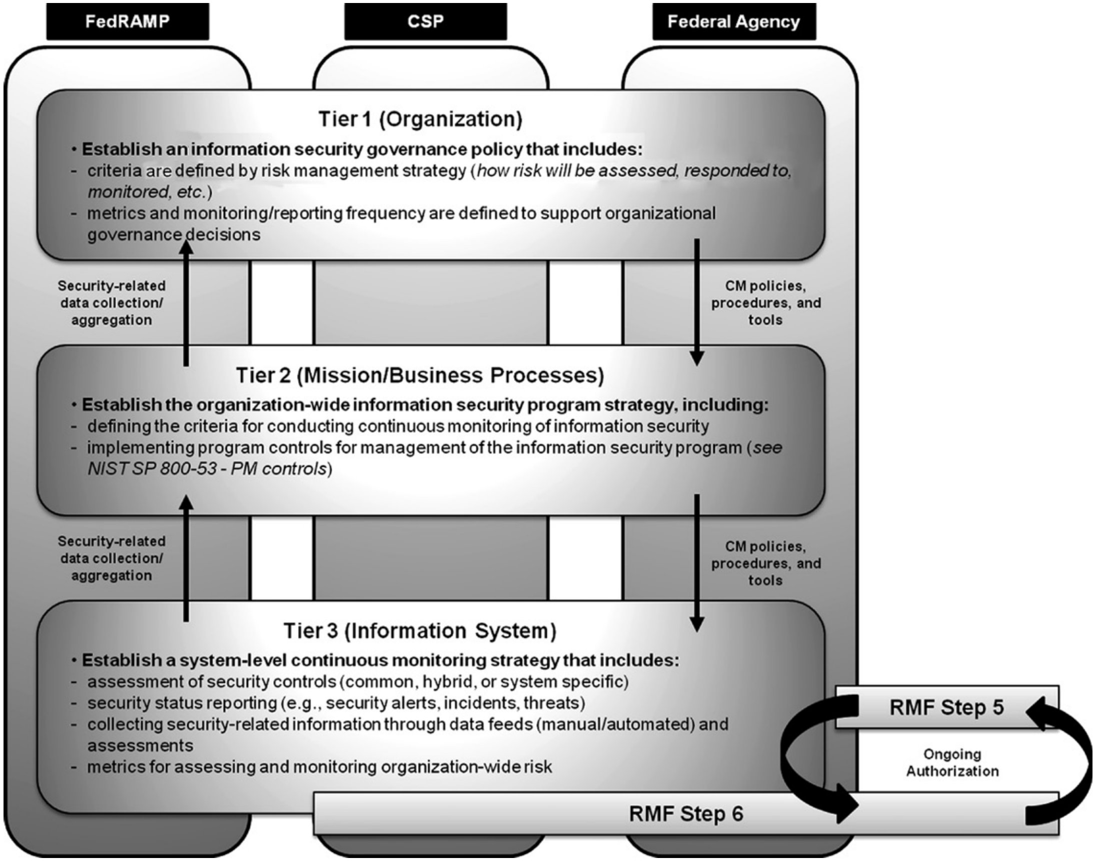

FedRAMP
CSP
Federal Agency
Tier 1 (Organization)
• Establish an information security governance policy that includes:
- criteria are defined by risk management strategy (how risk will be assessed, responded to, monitored, etc.)
- metrics and monitoring/reporting frequency are defined to support organizational governance decisions
Security-related data collection/ aggregation
CM policies, procedures, and tools
Tier 2 (Mission/Business Processes)
• Establish the organization-wide information security program strategy, including:
- defining the criteria for conducting continuous monitoring of information security
- implementing program controls for management of the information security program (see NIST SP 800-53 - PM controls)
Security-related data collection/ aggregation
CM policies, procedures, and tools
Tier 3 (Information System)
• Establish a system-level continuous monitoring strategy that includes:
- assessment of security controls (common, hybrid, or system specific)
- security status reporting (e.g., security alerts, incidents, threats)
- collecting security-related information through data feeds (manual/automated) and assessments
- metrics for assessing and monitoring organization-wide risk
RMF Step 5
Ongoing Authorization
RMF Step 6

FIGURE 11.3 Organization-Wide and FedRAMP Continuous Monitoring Activities

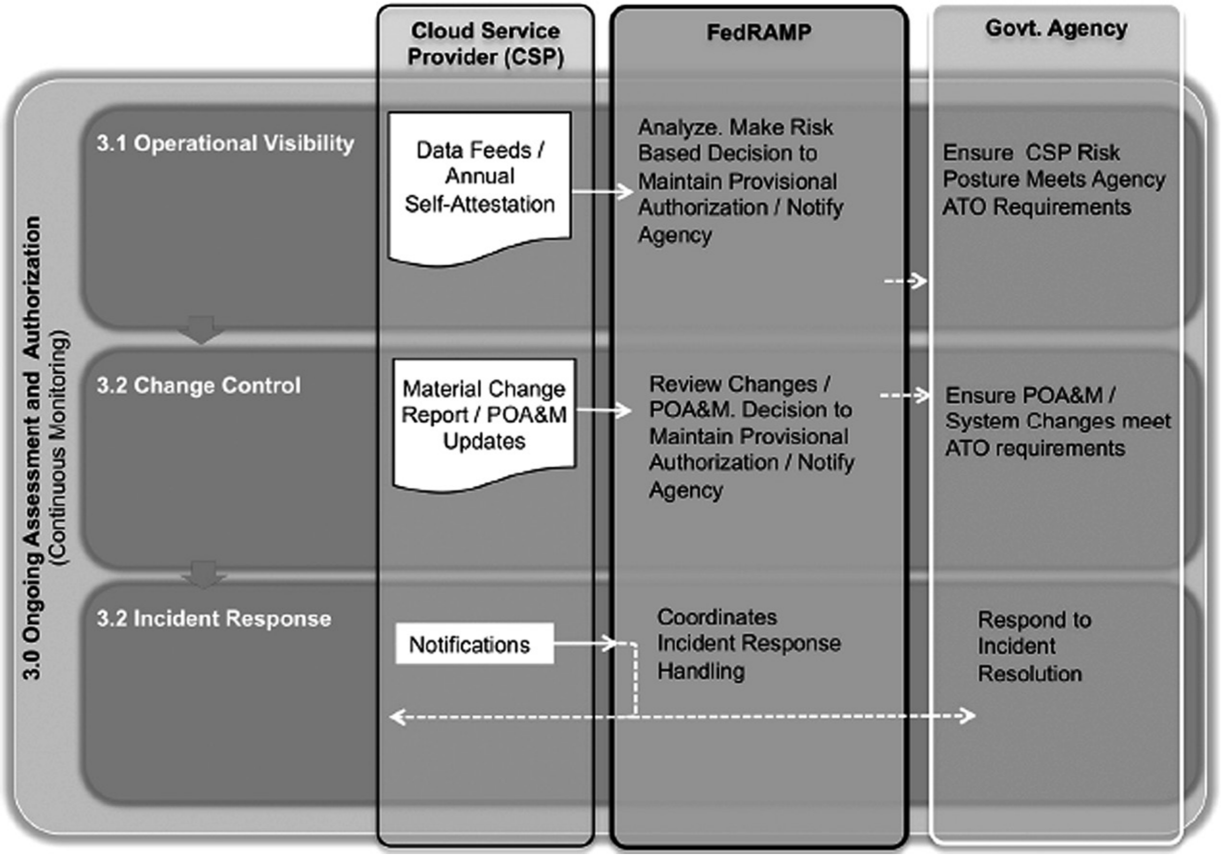

Cloud Service Provider (CSP)
FedRAMP
Govt. Agency
3.0 Ongoing Assessment and Authorization
(Continuous Monitoring)
3.1 Operational Visibility
Data Feeds / Annual Self-Attestation
Analyze. Make Risk Based Decision to Maintain Provisional Authorization / Notify Agency
Ensure CSP Risk Posture Meets Agency ATO Requirements
3.2 Change Control
Material Change Report / POA&M Updates
Review Changes / POA&M. Decision to Maintain Provisional Authorization / Notify Agency
Ensure POA&M / System Changes meet ATO requirements
3.2 Incident Response
Notifications
Coordinates Incident Response Handling
Respond to Incident Resolution

FIGURE 11.4 FedRAMP Continuous Monitoring [15]

security controls assessment and risk determination process into a dynamic process[61] that is supported by timely risk response actions and a cost-effective, ongoing authorization [2].

The FedRAMP security authorization process[62] focuses on integrating information security and risk management into the SDLC through the application of the NIST RMF. After the initial authorization, evidence of security control effectiveness will need to be obtained continuously to support the changes[63] within the cloud service and operating environment. The monitoring steps *(Step 6)* of the NIST RMF,[64] when aligned with the organization's CM and risk management activities, support the determination of risk at the organizational and mission/business tiers through system-level information.[65]

The operational visibility provides the transparency required by the FedRAMP PMO and federal agencies through the use of three sources of information: *data feeds (automated/manual)*, *annual security control assessment*, and *annual self-attestation*.[66] As we already discussed earlier in this chapter, federal agencies are required to submit monthly reporting on government-wide metrics to DHS. Data feeds produced by the CSP should be integrated into existing capabilities within the CSP's existing monitoring environment to align with the federal agency's reporting requirements. In addition to the CSP's continuous monitoring activities, Table 11.3 identifies an example list of artifacts that must be submitted to the FedRAMP PMO .

The change control process is enabled by monitoring and reporting activities. CM provides insight into the implementation of organizational- and information system–level policies, procedures, and secure configuration baselines. Monitoring[67] also identifies

[61] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Continuous monitoring of threats, vulnerabilities, and security control effectiveness provides situational awareness for risk-based support of ongoing authorization decisions."*

[62] The FedRAMP process is discussed in detail in Chapter 8, FedRAMP Primer.

[63] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Ongoing assessment of security control effectiveness supports a system's security authorization over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes."*

[64] The monitoring step is discussed in detail in Chapter 5, Applying the Risk Management Framework.

[65] From FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. *"CSPs provide different types of information: automated data feeds, periodically submitted specific control evidentiary artifacts, and annual self-attestation reports."*

[66] FedRAMP Program Management Office (PMO). Continuous Monitoring Strategy & Guide, Version 1.1. Washington: US General Services Administration; 2012. *"Delivery of continuous monitoring artifacts must be provided by the CSP as part of the annual self-attestation process. FedRAMP has developed a Self-Attestation Template and CSPs must fill out this template and provide named artifacts prior to reauthorization."*

[67] Security-focused configuration management includes four phases: *planning*, *identifying and implementing configurations*, *controlling configuration changes*, and *monitoring*.

Table 11.3 FedRAMP Continuous Monitoring Deliverables [13]

Security Control	Frequency	Deliverable	Description
IR-6—Incident Reporting	Continuous and Ongoing	• Self-Attestation	• CSPs should notify of new incidents as they are discovered. • CSPs to include a summary of reported incidents. • CSPs should fill out Incident Report Forms as needed.
RA-5a—Vulnerability Scanning	Monthly	• Vulnerability Scan Results	• CSPs must scan operating systems/infrastructure monthly. All scan reports must be sent to the ISSO.
CA-5—Plan of Action and Milestones	Quarterly	• Updates to POA&Ms	• CSPs should update POA&Ms based on the findings from security assessments, security impact analyses, risk assessments, continuous monitoring activities, and any other indications of a security leak. • CSPs must update the POA&M as needed, and must submit it to the ISSO quarterly.
RA-5a—Vulnerability Scanning	Quarterly	• Vulnerability Scan Results	• CSPs must scan web applications and databases quarterly scan reports should be sent to the ISSO.
XX-1—Information Security Policies	Annual	• Self-Attestation	• CSPs must review Information Security Policies and Procedures annually. Insert the updated Policy document as an Attachment to the System Security Plan and submit the updated plan to the ISSO one year from the Provisional Authorization date and each year thereafter.
CA-2b-Security Assessments	Annually	• Self-Attestation	• CSPs must have a 3PAO assess a subset of their security controls annually. Submit the assessment report to the ISSO one year from the Provisional Authorization date and each year thereafter.

Table 11.3 FedRAMP Continuous Monitoring Deliverables [13] (*continued*)

Security Control	Frequency	Deliverable	Description
CA-7(2)—Continuous Monitoring	Annually	• Self-Attestation	• CSPs must require unannounced penetration testing to occur annually to ensure compliance with all vulnerability mitigation procedures. All penetration testing reports must be sent to the ISSO.
CM-9—*Configuration Management Plan*	Annual	• Self-Attestation	• CSPs must review and update the Configuration Management Plan annually. Submit the new plan to the ISSO at the time of annual Self-Attestation one year from the Provisional Authorization date (and each year thereafter).
CP-2d—Contingency Plan	Annual	• Self-Attestation	• CSPs must review and update the *IT Contingency Plan* annually. Submit the new plan to the ISSO at the time of annual Self-Attestation one year from the Provisional Authorization date (and each year thereafter).
CP-4a—Contingency Plan Testing (*Moderate Systems Only*)	Annual	• Self-Attestation	• CSPs must test and exercise the *IT Contingency Plan* (for moderate impact systems) every year. • CSPs must insert a new IT Contingency Plan Test Report into Appendix F of the IT Contingency Plan (which is submitted annually). • CSPs with moderate cloud services are required to perform functional testing and exercises.

Table 11.3 FedRAMP Continuous Monitoring Deliverables [13] (*continued*)

Security Control	**Frequency**	**Deliverable**	**Description**
IR-3—Incident Response Testing	Annual	• Self-Attestation	• CSPs must perform incident response testing annually. When the *System Security Plan* is updated annually, record the results of the incident response testing directly in the control description box indicating when testing took place, testing materials, who participated, and who conducted the testing. • CSPs should test all contact information in the Appendices of the *Incident Response Plan* to make sure they are accurate.
IR-8c—Incident Response Plan	Annual	• Self-Attestation	• CSPs must review the *Incident Response Plan* annually and update it if necessary. • CSPs should insert the updated Incident Response Plan as an attachment to the *System Security Plan.*
PL-2b,c—System Security Plan	Annual	• Self-Attestation	• CSPS must update Table 9.1 in the *System Security Plan*. • CSPs must review and update their System Security Plan (SSP) annually.
RA-5a - Security Assessments	Annually	• Vulnerability Scan Results	• CSPs must have an accredited 3PAO scan operating systems/infrastructure, web applications, and databases annually. All scan reports must be sent to the ISSO.

Table 11.3 FedRAMP Continuous Monitoring Deliverables [13] (*continued*)

Security Control	Frequency	Deliverable	Description
CP-4a—Contingency Plan Testing	Every Three Years	• Self-Attestation	• CSPs should test and exercise the *IT Contingency Plan* (for low-impact systems—every three years through a tabletop exercise; for moderate-impact system—annually through a functional exercise). • CSPs should add weaknesses and deficiencies identified through the contingency plan testing to the POA&Ms. • CSPs should record the testing date in the *System Security Plan* and submit the test results with the annual Self-Attestation.
AT-4b—Security Training Records	Every Three Years	• Self-Attestation	• CSPs must archive security training records for three years. In the *System Security Plan*, record who participated in training and when the training took place. Archive the actual training materials. • CSPs should identify the personnel that have been trained, the dates they were trained, and the subject areas that training covered in the training records.

undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes [14]. The CSP's Configuration Management Plan (CMP) is an essential tool for identifying and communicating changes to the cloud service and any potential impacts to the security and risk posture. Through a security impact analysis,[68] changes can be analyzed (or assessed through the annual assessment activities) to determine if the existing security controls would impact the federal agencies' risk tolerance.

[68] NIST Special Publication (SP) 800-128, Appendix I, *Guide for Security-Focused Configuration Management of Information Systems,* contains a sample security impact worksheet.

Incident response is a critical component of the FedRAMP CM process. A security incident[69] should be anticipated and response planned. The Incident Response Plan (IRP) documents the CSP's implementation of the incident response life cycle[70] that includes activities for the detection and analysis of and response to a security incident. In the event of a security incident, the CSP has the responsibility to notify[71] the United States Computer Emergency Readiness Team (US-CERT) and the affected federal agency. The FedRAMP PMO and US-CERT will then coordinate response efforts across the impacted federal agencies, including conducting a forensic analysis through a root cause determination and providing recommended remediation actions [12].

SUMMARY

In this chapter, CM was discussed from the perspective of the organization supporting the monitoring and assessment activities. CM includes both strategic and tactical components that enable it to be implemented cost-effectively. Beginning with a comprehensive and robust CM strategy, the organization can ensure alignment with the organization's overall risk management strategy. The design and implementation of the CM program is supported through the definition of metrics, frequencies, and formats for assembling and distributing security-related information. Within the context of FedRAMP, CM can be a complex activity that requires the appropriate coordination between multiple stakeholders. The interaction between the CSP, FedRAMP PMO, and federal agency relies upon the consistent implementation of policies, procedures, processes, and templates that support activities that enable operational visibility, change control, and incident response.

References

[1] Guttman B, Rockback E. NIST Special Publication (SP) 800-12, an introduction to computer security: The NIST handbook. Maryland: National Institute of Standards and Technology; 1995.

[2] Dempsey K, Nirali C, Johnson A, Johnston R, Jones A, Orebaugh A et al. NIST Special Publication (SP) 800-137, Information security continuous monitoring (ISCM) for federal information systems and organizations. Maryland: National Institute of Standards and Technology; 2011.

[69] NIST Special Publication (SP) 800-61 Revision 2, *"A computer security incident is a violation or imminent threat of violation1 of computer security policies, acceptable use policies, or standard security practices."*

[70] NIST Special Publication (SP) 800-61 Revision 2, *Computer Security Incident Handling,* describes the incident response life cycle to support *containment*, *eradication*, and *recovery*.

[71] *US-CERT Incident Reporting System*. Available from: https://forms.us-cert.gov/report.

[3] GPRA Modernization Act of 2010 [Internet]. Washington: US Government Printing Office; [cited April 28, 2012]. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ352/pdf/PLAW-111publ352.pdf>.

[4] Lew J. Office of Management and Budget (OMB) Memorandum 11-33, FY 2011 reporting instructions for the federal information system management act and agency privacy management. Washington: Executive Office of the President, Office of Management and Budget; 2011.

[5] Lew J. Office of Management and Budget (OMB) Memorandum 10-28, Clarifying cybersecurity responsibilities and activities of the executive office of the president and the department of homeland security (DHS). Washington: Executive Office of the President, Office of Management and Budget; 2010.

[6] Office of Management and Budget (OMB). Fiscal Year 2011 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002. Washington: Executive Office of the President, Office of Management and Budget; 2012.

[7] Coose M. Federal Continuous Monitoring Working Group (Draft) Presentation. Washington: US Department of Homeland Security; 2011.

[8] Joint task force transformation initiative. NIST Special Publication (SP) 800-53 Revision 4, Security and privacy controls for federal information systems and organizations. Maryland: National Institute of Standards and Technology; 2012.

[9] US Department of Homeland Security, Federal Network Security Branch. FY 2012 Chief Information Officer, Federal Information Security Management Act reporting metrics. Washington: US Department of Homeland Security; 2012.

[10] Williams-Bridgers J. State has taken steps to implement a continuous monitoring application, but key challenges remain. Washington: US Government Accountability Office; 2011.

[11] US Department of Homeland Security, Federal Network Security Branch. Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) reference architecture report version 1.8. Washington: US Department of Homeland Security; 2010.

[12] FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) version 1.0. Washington: US General Services Administration; 2012.

[13] FedRAMP Program Management Office (OMB) Office. FedRAMP continuous monitoring strategy and guide. Washington: US General Services Administration; 2012.

[14] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D. NIST Special Publication (SP) 800-128, Guide for security-focused configuration management of information systems. Maryland: National Institute of Standards and Technology; 2011.

[15] FedRAMP Program Management Office (PMO), FedRAMP Concept of Operations (CONOPS) version 1.1. Washington: US General Services Administration; 2012.

CHAPTER

Cost-Effective Compliance Using Security Automation 12

INFORMATION IN THIS CHAPTER:

- Introduction
- CM Reference Architectures
- Security Automation Standards and Specifications
- Operational Visibility and Continuous Monitoring

INTRODUCTION

Security automation is an essential part of an information security program, enabling organizations to achieve more efficiency in monitoring activities. Not all continuous monitoring (CM) can be accomplished through automation. However, where automation is applied, an organization can more cost-effectively monitor and continually assess security controls. The result of using security automation enhances the security-related information produced from monitoring activities, offering a more accurate measure of the state of the organization's security posture. Security automation is supported by the metrics established by the organization for the collection and analysis of the needed security-related information. This information becomes a valuable input into the organization's risk management function, thereby enabling the organization's management to realize "*near real-time*," risk-based decision-making.

Tools and technologies used in CM provide the organization with insight into the security controls that can be automated. However, in some circumstances manual monitoring may still be required in the organization's security program. This is important to note, because manual monitoring can still serve as a viable option, specifically in cases where the organization's CM strategy is still maturing and metrics required for the collection of information are largely undefined.

The CM strategy should address the *people*, *processes*, *technologies* and the *environment*. In addition, the CM strategy does not focus solely on the security-related information that is easy for an organization to collect or easy to automate [1]. Therefore, where automation is used, the organization will also need to ensure the strategy reflects its role to ensure it achieves the desired efficiency in obtaining

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00012-5

outcome-oriented results. For example, where large volumes of security-related information are collected, automation augments existing processes by reducing the burden and potential errors associated with the human aspects[1] of conducting analysis. Automation also supports the organization by interpreting[2] the collected data to enable stakeholders to make more informed, risk-based decisions.

Automation is not a replacement for the human element in an information security program. The application of automation within an organization's CM strategy should be linked to the existing processes (or new processes[3] where gaps exist) to ensure the organization understands the associated impact in the potential loss of visibility and efficiency due to a compromise in the tools and technologies relied upon when making risk-based decisions. This will also guide the organization in ensuring any automation that is used to supplement monitoring capabilities[4] within the information security program is appropriately protected.

As illustrated in Figure 12.1, CM plays a critical role in the organization's risk management strategy. The use of automated tools facilitates the collection of "a larger and more diverse pool of technologies, people, processes, and environments" [1]. However, the selection of the tools and technologies should be considered only after the organization has thoroughly defined the metrics that the organization will use as a basis for analyzing and responding[5] to findings through the organization's risk management processes. Through the development of metrics, the organization

[1] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Automation serves to augment the security processes conducted by security professionals within an organization and may reduce the amount of time a security professional must spend on doing redundant tasks, thereby increasing the amount of time the trained professional may spend on tasks requiring human cognition."*

[2] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Automated tools are often able to recognize patterns and relationships that may escape the notice of human analysts, especially when the analysis is performed on large volumes of data."*

[3] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Tools operate within the context of processes designed, run, and maintained by humans."*

[4] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"During security control implementation (RMF Step 3), consideration is given to the capabilities inherent in available technology to support ISCM as part of the criteria in determining how best to implement a given control."*

[5] From Dempsey, K., Nirali, C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"Response to findings at all tiers may include risk mitigation, risk acceptance, risk avoidance/rejection, or risk sharing/transfer, in accordance with organizational risk tolerance."*

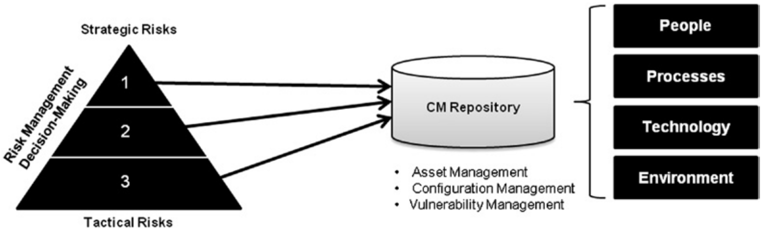


FIGURE 12.1 Automating CM Activities

TIP

Tools and technologies enhance CM activities. Several considerations [1] when selecting tools and technologies to support automation capabilities include:

- Collection sources.[6]
- Open specification support (e.g., SCAP[7]).
- Interoperability.
- Reporting.
- Data aggregation.

can identify the tools and technologies that present the necessary information at a frequency consistent with those defined in the strategy.

This chapter will focus on CM reference architectures developed to support the identification of tools and technologies that enable organizations to automate different aspects of CM (i.e., gathering, aggregating, analyzing, and reporting). Additionally, existing and emerging security automation standards and specifications will be briefly discussed as a means of addressing the importance of standardization in the reporting and the exchange of data when organizations implement security automation in CM-related activities.

CM REFERENCE ARCHITECTURES

A CM reference architecture is an abstract depiction of the components and interfaces that must exist within a CM implementation. It operates as a template which can be customized through a specific set of CM solutions. In addition, using a CM reference architecture, such as those that will be discussed in this section, assists organizations

[6] From Dempsey, K., Nirali C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *”Automation supports collecting more data more frequently and from a larger and more diverse pool of technologies, people, processes, and environments.”*

[7] *Security Content Automation Protocol (SCAP)*. Available from: http://scap.nist.gov/.

in selecting the tools and technologies that can be used to efficiently and effectively gather, aggregate, analyze and report data collected through CM activities.

Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture

As mentioned in Chapter 11, the US Department of Homeland Security (DHS), Federal Network Security (FNS) Branch, developed a reference architecture that provided an abstraction of a security posture monitoring and risk scoring system, that is informed by computing and network asset that can be used by other federal agencies seeking to apply risk scoring principles to their information security program [2]. The DHS FNS Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS)[8] provided the initial framework for implementing monitoring process and for establishing requirements for automated tool selection and integration. For completeness and for illustration purposes, Figure 12.2 provides a view of the CAESAR subsystems. In the next section, the follow-on reference architecture CAESARS Framework Extension (FE) developed by NIST, an enterprise continuously monitoring technical reference model, will be discussed with additional detail as it relates to supporting automation in a CM program.

CAESARS Framework Extension Reference Architecture

The CAESARS FE is an enhanced version of the CM reference architecture developed by DHS. The specific differences will not be discussed in this chapter, but it is important to note that the essential characteristics have remained the same, with differences focused on adding additional functionality, granularity within subsystem specifications, and to further leverage existing and emerging security automation standards [3]. The CAESARS FE is a conceptual model used to enable the real-time capabilities of the NIST Risk Management Framework (RMF)[9] with specific emphasis placed on automating continuous monitoring *Step 6* functions. Through an elaboration of a technical architecture using the model presented in the CAESARS FE, tools and technologies can be developed that facilitate CM within an enterprise and make information available to support risk-based decision-making.

In this section, the subsystems and components, and specifications will be briefly discussed, followed by a description of how the application of the CAESAR FE technical reference model supports each of the data domains.[10] Although a specific

[8] *FNS CAESARS References Architecture*. Available from: www.dhs.gov/xlibrary/assets/fns-caesars.pdf.
[9] NIST RMF is discussed in detail in Chapter 5, Applying the Risk Management Framework.
[10] From Waltermire, D., Halbardier, A., Humenansky, A., Mell, P. NIST Interagency Report (IR) 7800 (Draft), Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains. Maryland: National Institute of Standards and Technology; 2012. *"A specific class of cyber security data, methodologies, and procedures."*

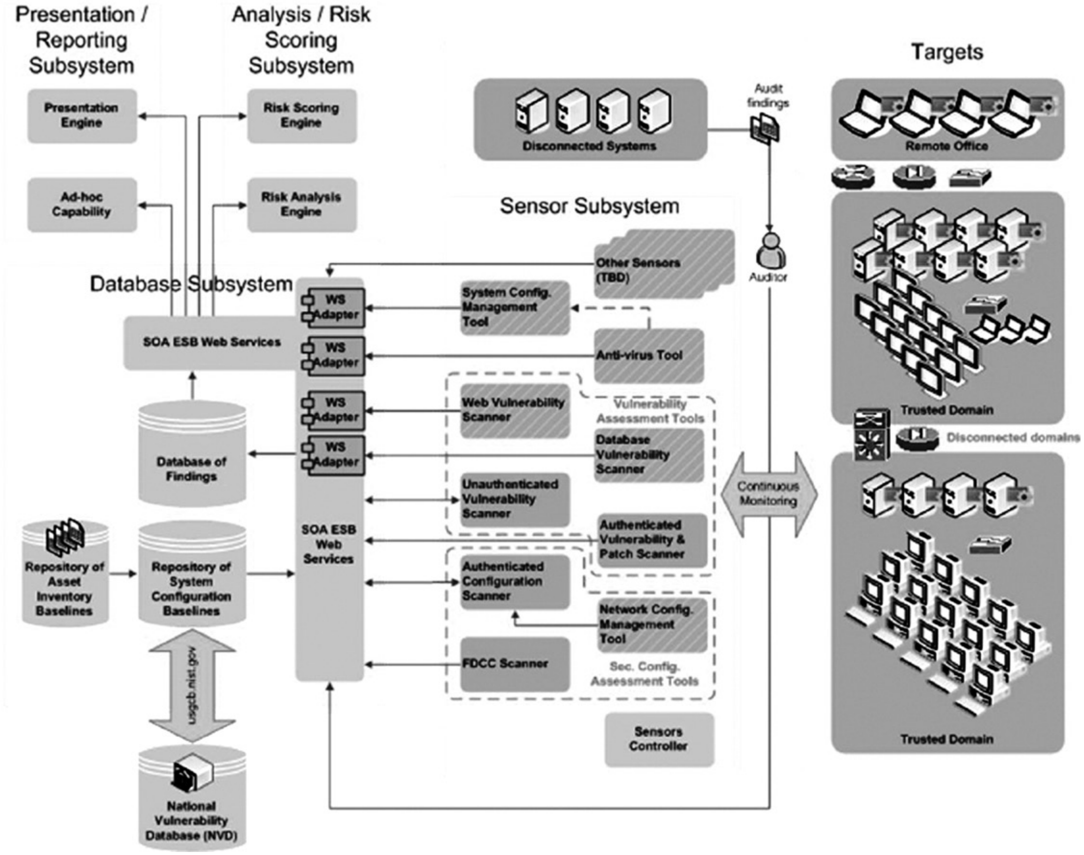

Presentation / Reporting Subsystem
Presentation Engine
Ad-hoc Capability
Analysis / Risk Scoring Subsystem
Risk Scoring Engine
Risk Analysis Engine
Database Subsystem
SOA ESB Web Services
Database of Findings
Repository of Asset Inventory Baselines
Repository of System Configuration Baselines
usgcb.nist.gov
National Vulnerability Database (NVD)
WS Adapter
WS Adapter
WS Adapter
WS Adapter
SOA ESB Web Services
Disconnected Systems
Audit findings
Auditor
Sensor Subsystem
Other Sensors (TBD)
System Config. Management Tool
Anti-virus Tool
Web Vulnerability Scanner
Vulnerability Assessment Tools
Database Vulnerability Scanner
Unauthenticated Vulnerability Scanner
Authenticated Vulnerability & Patch Scanner
Authenticated Configuration Scanner
Network Config. Management Tool
FDCC Scanner
Sec. Config. Assessment Tools
Sensors Controller
Continuous Monitoring
Targets
Remote Office
Trusted Domain
Disconnected domains
Trusted Domain

FIGURE 12.2 Automating CM Activities [2]

Table 12.1 Security Automation Domains [1]

Domain	Security Controls[a]	
Vulnerability and Patch Management	• CA-2—Security Assessments • CA-7—Continuous Monitoring • CM-3—Configuration Change Control • IR-4—Incident Handling • IR-5—Incident Monitoring	• MA-2—Controlled Maintenance • RA-5—Vulnerability Scanning • SA-11—Developer Security Testing • SI-2—Flaw Remediation • SI-11—Error Handling
Event and Incident Management ([1]Logging Only, [2]IDPS Only, *Both)	• AC-4—Information Flow Enforcement[2] • AC-17—Remote Access[2] • AC-18—Wireless Access[2] • AU-2—Auditable Events* • AU-3—Content of Audit Records[1] • AU-6—Audit Review, Analysis, and Reporting* • AU-7—Audit Reduction and Report Generation[1] • AU-8—Time Stamps[1] • AU-12—Audit Generation*	• AU-13—Monitoring for Information Disclosure[2] • CA-2—Security Assessments* • CA-7—Continuous Monitoring* • IR-5—Incident Monitoring[1] • RA-3—Risk Assessment* SI-4—Information System Monitoring* • SC-7—Boundary Protection[2] • SI-3—Malicious Code Protection[2] • SI-7—Software and Information Integrity[2]
Malware Detection	• CA-2—Security Assessments • CA-7—Continuous Monitoring • IR-5—Incident Monitoring • RA-3—Risk Assessment • SA-12—Supply Chain Protection • SA-13—Trustworthiness	• SI-3—Malicious Code Protection • SI-4—Information System Monitoring • SI-7—Software and Information Integrity • SI-8—Spam Protection
Asset Management	• CA-7—Continuous Monitoring • CM-2—Baseline Configuration • CM-3—Configuration Change Control	• CM-8—Information System Component Inventory • SA-10—Developer Configuration Management

Table 12.1 Security Automation Domains [1] (*Continued*)

Domain	Security Controls[a]	
Configuration Management	• AC-2—Account Management • AC-3—Access Enforcement • AC-5—Separation of Duties • AC-7—Unsuccessful Login Attempts • AC-9—Previous Logon (Access) Notification • AC-10—Concurrent Session Control • AC-11—Session Lock • AC-19—Access Control for Mobile Devices • AC-20—Use of External Information Systems • AC-22—Flaw Remediation • CA-2—Security Assessments • CA-7—Continuous Monitoring • CM-2—Baseline Configuration • CM-3—Configuration Change Control • CM-5—Access Restrictions for Change	• CM-6—Configuration Settings • CM-7—Least Functionality • IA-2—Identification and Authentication (Organizational Users) • IA-3—Device Identification and Authentication • IA-4—Identifier Management • IA-5—Authenticator Management • IA-8—Identification and Authentication (Non-Organizational Users) • IR-5—Incident Monitoring • MA-5—Maintenance Personnel • PE-3—Physical Access Control • RA-3—Risk Assessment • SA-7—User-Installed Software • SA-10—Developer Configuration Management • SI-2—Flaw Remediation
Network Management	• AC-4—Information Flow Enforcement • AC-17—Remote Access • AC-18—Wireless Access • CA-7—Continuous Monitoring • CM-2—Baseline Configuration • CM-3—Configuration Change Control • CM-4—Security Impact Analysis • CM-6—Configuration Settings	• CM-8—Information System Component Inventory • SC-2—Application Partitioning • SC-5—Denial of Service Protection • SC-7—Boundary Protection • SC-10—Network Disconnect • SC-32—Information System Partitioning • SI-4—Information System Monitoring

Table 12.1 Security Automation Domains [1] (*Continued*)

Domain	Security Controls[a]
License Management	• CA-7—Continuous Monitoring • CM-8—Information System Component Inventory • SA-6—Software Usage Restrictions
Information Management	• AC-4—Information Flow Enforcement • AC-17—Remote Access • CA-3—Information System Connections • CA-7—Continuous Monitoring • SC-9—Transmission Confidentiality • SI-12—Information Output Handling and Retention
Software Assurance	• CA-7—Continuous Monitoring • SA-4—Acquisition • SA-8—Security Engineering Principles • SA-11—Developer Security Testing • SA-12—Supply Chain Protection • SA-13—Trustworthiness • SA-14—Critical Information System Components • SI-13—Predictable Failure Prevention

[a] *Security automation domains cover 63 of the total 189 available controls in NIST SP 800-53 Revision 3 (excludes low, moderate, and high baselines).*

discussion of security automation domains[11] is beyond the scope of this book, it is important to list those domains identified [1] that require support by the CM reference technical model[12] as shown in Table 12.1.

Subsystems and Components

The CAESARS FE reference architecture consists of six subsystems. Each subsystem, as depicted in Figure 12.3, contains one or more components that provide a specific function or capability (e.g., analysis and scoring, collection, content management, etc.).

[11] From Dempsey, K., Nirali C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *"A security automation domain is an information security area that includes a grouping of tools, technologies, and data. Data within the domains is captured, correlated, analyzed, and reported to present the security status of the organization that is represented by the domains monitored."*

[12] From Dempsey, K., Nirali C., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., et al. NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Maryland: National Institute of Standards and Technology; 2011. *The tools support these domains need to be instrumented to interface with CM solutions (i.e. external systems instrumented for CM integration).*

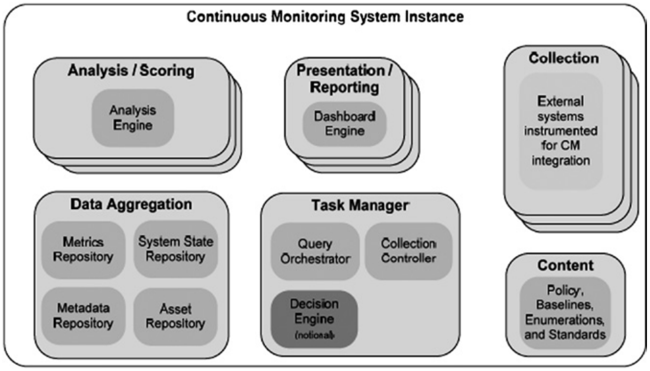


FIGURE 12.3 CAESARS FE Subsystems and Components [3]

The subsystems and components are meant to be independent and security tool and technology agnostic. Therefore, it is important to understand the intent of the subsystems and components to enable organizations to apply the technical reference model in a way that will assist in identifying and implementing CM capabilities that result in a solution that cost-effectively supports the CM requirements. Below is an overview of each of the subsystems and components:

- The *presentation/reporting* subsystem, consisting of the *dashboard engine*, is the source for user input/outputs. Within the CM system instance, this subsystem would primarily interface with the task manager subsystem using queries designed to fulfill user requests for security-related information.
- The *task manager* subsystem performs the orchestration in the CM system instance between the analysis/scoring, data aggregation, presentation/reporting, and collection subsystems. This subsystem performs the orchestration through use of several components, such as the *query orchestration*, *collection controller*, and *decision engine*.
- The *collection* subsystem collects data based on a user query (task manager), using content that describes the organization's policies (content), and stores the results (data aggregation). When a multi-tiered[13] CM capability is used, as illustrated in Figure 12.4, a collection subsystem may not exist within all of the CM instances.[14] It is also important to highlight that a collection subsystem is

[13] From Mell, P., Waltermire, D., Feldman, L., Booth, H., Regland, Z., Ouyang, A., et al. NIST Interagency Report (IR) 7756 (Second Draft), CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model. Maryland: National Institute of Standards and Technology; 2012. *In a multi-tiered CM situation, a CM instance higher in the hierarchy may not have any assets to monitor, but instead rely upon data feeds from lower tier CM instances.*

[14] More than one CM instance can be used in organizations that have a need to structure the CM implementation organization-wide to support the different tiers of decision-makers within the CM program (e.g., tier 1—governance, tier 2—mission/business processes, and tier 3—information system).

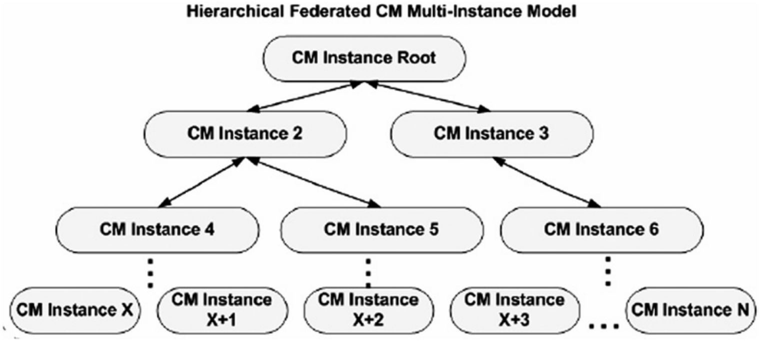


FIGURE 12.4 Multi-Tiered, Hierarchical CM Implementation [3]

not a core component of the CM implementation and could be an external system that interfaces with a CM instance.

- The *data aggregation* subsystem is the central repository for data (e.g., raw, analyzed, etc.). This subsystem consists of multiple repositories: *system state*, *asset*, *metrics*, and *metadata*. The data aggregation subsystem interfaces with other subsystems such as input from the collection subsystem for storage of raw collected data, raw data retrieval and analyzed data storage from the analysis/scoring subsystem, and query result storage from task managers that exist in lower-tiers in a multi-tiered hierarchical model [3] (see Figure 12.3).
- The *analysis/scoring* subsystem provides the analysis and scoring function within the CM implementation, potentially supporting multiple scoring methodologies *analysis engine* components. This subsystem is a critical component of the CM implementation. It receives queries from the task manager subsystem, retrieves and stores data in the data aggregation subsystem, and obtains scoring algorithms, parameters, and associated scoring data from the content subsystem [3].
- Finally, the *content* subsystem maintains the organizational policies which are used to compare system state. The primary purpose of this subsystem is to maintain the policies (e.g., security baselines configurations) and supporting data (e.g., enumeration of products being evaluated, or vulnerabilities being identified) that are used by the collection subsystem(s) or the analysis/risk scoring subsystem(s). Since an organization may have a single source for storing organizational policies, only one content subsystem would be required for an entire CM implementation to enable sharing among the different CM instances.

Specifications: Workflows, Subsystems, and Interfaces

The CAESARS FE technical specification consists of the workflows, subsystems, and interfaces that enable the implementation of the CM reference model. The *workflows* specifications define the “coordinated operations of all the subsystems and components within the model” [4]. The *subsystem* specifications enable subsystems to operate as independent and tool agnostic, "plug-in-play" modules that are interoperable between CM implementations. Since subsystems perform an independent role within the CM implementation, clearly defining the required functionality at a "generic" level enables easier integration of different products/services. The last specification, the *interfaces*, plays an essential role in bridging the communication between the individual subsystems and facilitating workflow interactions.

This section is not intended to provide a detailed description of these specifications, but instead to provide a general overview to expand the discussion of the CAESARS FE as a technical reference model for identifying tools and technologies that can be integrated into CM solutions to assist CSPs in addressing the FedRAMP operational visibility and other CM requirements. Through the selection of CSPs that implement the specifications, federal agencies can focus on continuously monitoring security-related information across the enterprise (i.e., hardware, software, and services) under a single governance structure to include those mission/business processes that have been extended to the cloud service environment.[15]

Specification Layers

The CAESARS FE consists of multiple layers that extend from a high-level reference model description to a technical specification that links the CM implementation to a specific data domain (e.g., asset management, configuration management, and vulnerability management). As illustrated in Figure 12.5, the layers of the CM specifications extend from layer 5 where the subsystem and interconnections[16] are defined, to layer 4 which addresses specifications for describing the workflows, subsystems, and interfaces,[17] to the actual binding of the technical reference model to data domains in layer 2.[18] Layers 3 and 1 are beyond the scope of this book.

Workflows

As described earlier, workflows provide coordinated operations for moving data within the CM technical reference model. Workflows describe specific use cases that are driven by the necessity for different subsystems and components to interoperate

[15] DHS/FNS is in the process of establishing technical requirements for the Continuous Diagnostic and Mitigation (CDM) Program which will provide federal agencies and state and local governments with the ability to enhance and automate their existing continuous network monitoring capabilities, correlate and analyze critical security-related information, and strengthen risk-based decision making at the agency and federal enterprise level. Available from: https://www.fbo.gov/utils/view?id=ae650dd0661deab13c6805f94a542a25.

[16] NIST Interagency Report (IR) 7756 (Second Draft), *"CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model."* Available from: http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf.

[17] NIST Interagency Report (IR) 7799 (Draft), *Continuous Monitoring Reference Model Workflow, Subsystem, and Interface Specifications.* Available from: http://csrc.nist.gov/publications/drafts/nistir-7799/Draft-NISTIR-7799.pdf.

[18] NIST Interagency Report (IR) 7800 (Draft), *Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains.* Available from: http://csrc.nist.gov/publications/drafts/nistir-7800/Draft-NISTIR-7800.pdf.

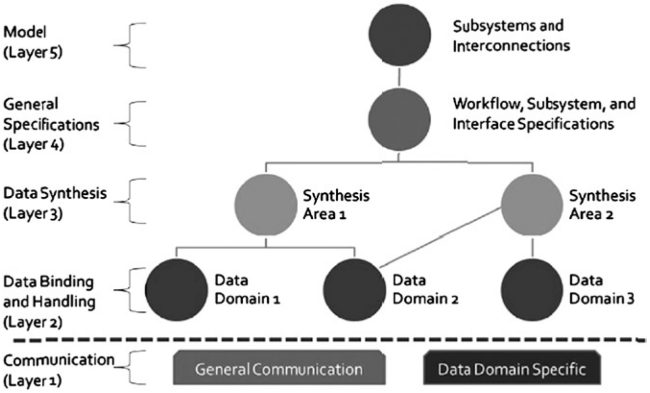


FIGURE 12.5 CAESAR FE Specification Layers [4]

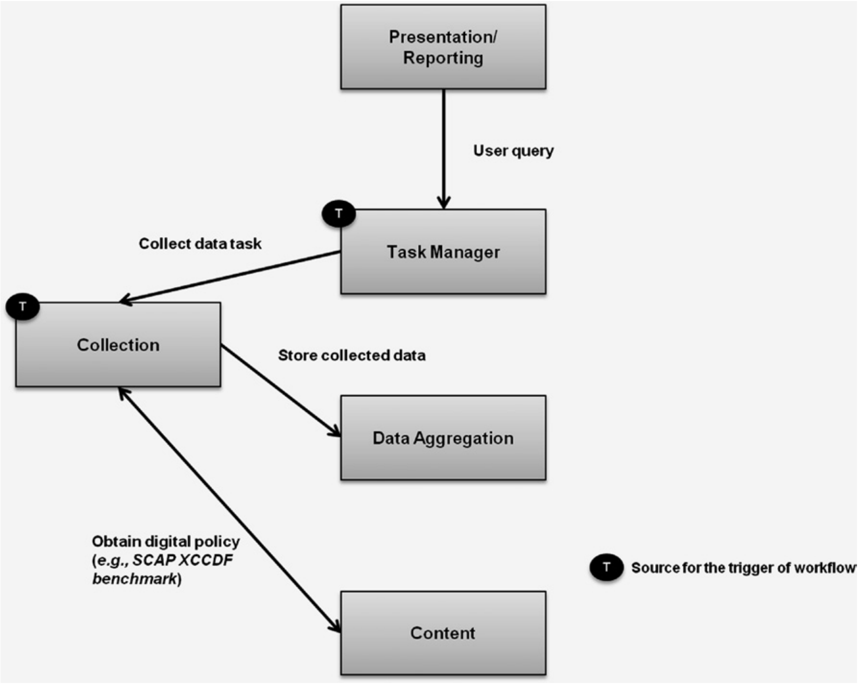


FIGURE 12.6 Example Data Acquisition Workflow

to perform a specific function (e.g., acquiring data through collection and reporting, fulfilling queries requests). For example a workflow for the data acquisition involves the collection subsystem interacting with other subsystems to support the acquisition of data. Figure 12.6 provides an illustration for how this workflow would be executed in a CM implementation. Omitted from the diagram is specific component interaction within the workflow. Since components within a subsystem collectively support the subsystem's implementation of a specific requirement within a workflow (e.g., collection controller initiating a task to the collection subsystem to collect data would be sent by the task manager), the actions of components have been abstracted to the subsystem-level.

Subsystems

The subsystem specifications provide a detailed description of the requirements that must be supported by a specific subsystem to effectively implement the CM technical reference model. Since the specifications are data domain agnostic, they are not specifically linked with a specific monitoring domain (i.e., asset management, configuration management, vulnerability management). Instead, the specifications describe the capabilities that must be supported by individual components. For example, the collection controller within the task manager subsystem provides the capability to process tasks (*task processing*[19]) and initiate data collection tasks (*subtask propagation*[20]) [4]. For the task manager to support the ability to initiate a task to request the collection of data from a user query, the task manager needs to be able to support multiple capabilities offered through these discrete services that interact within the CM implementation to support workflows.

Interfaces

Interface specifications provide the standardized mechanism in which subsystems can effectively communicate with each other and enable them to operate as independent modules that, when collectively implemented, support the entire CM technical reference model. Interfaces are exposed through Web Services Definition Language (WSDL)[21] that describes the web services implemented within the subsystem(s) where the interface exists. For example, Figure 12.7 provides an oversimplified illustration of the "Results Reporting" interface that is implemented by the Data Aggregation subsystem which enables other subsystems and components to send asset information for storage [4]. The WSDL describes the services(s) that are supported

[19] From Mell, P., Waltermire, D., Halbardier, A., Feldman, L. NIST Interagency Report (IR) 7799 (Draft), Continuous Monitoring Reference Model Workflow, and Specifications. Maryland: National Institute of Standards and Technology; 2012. *"The Collection Controller can receive incoming tasks, manage data collection fulfillment, and respond with completion status."*

[20] From Mell, P., Waltermire, D., Halbardier, A., Feldman, L. NIST Interagency Report (IR) 7799 (Draft), Continuous Monitoring Reference Model Workflow, and Specifications. Maryland: National Institute of Standards and Technology; 2012. *"The Collection Controller can propagate data collection tasking to the appropriate Collection subsystems and keep track of their completion."*

[21] *Web Services Description Language (WSDL)*. Available from: http://www.w3.org/TR/wsdl.

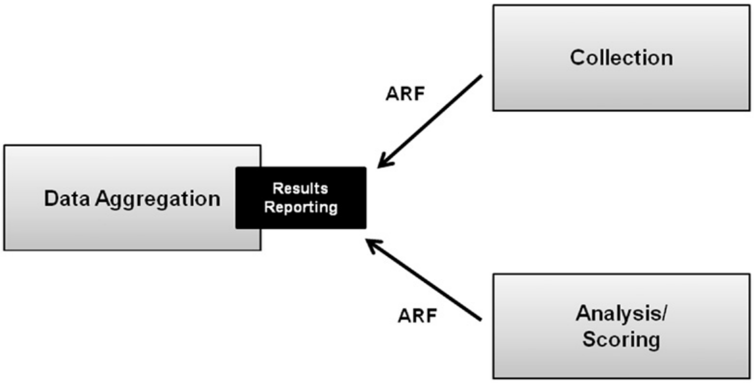


FIGURE 12.7 Results Reporting Interface

by the interface and the requirements for sending the asset[22] information (e.g., Asset Reporting Format (ARF)[23]).

SECURITY AUTOMATION STANDARDS AND SPECIFICATIONS

The implementation of CM requires using tools and technologies that are based on standards and specifications that are open and industry-supported. Standards and specifications provide a foundation for implementing automation that promotes portability and interoperability across tool sets and domain boundaries. As discussed earlier, the layer 2 in the CAESARS FE technical reference model binds the reference model to data domains (e.g., asset management,[24] configuration management,[25]

[22] From Halbardier, A., Waltermire, D., Johnson, M. NIST Interagency Report (IR) 7694, Specification for the Asset Reporting Format 1.1. Maryland: National Institute of Standards and Technology; 2011. *"Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g. locks, cabinets, keyboards)."*

[23] From Halbardier, A., Waltermire, D., Johnson, M. NIST Interagency Report (IR) 7694, Specification for the Asset Reporting Format 1.1. Maryland: National Institute of Standards and Technology; 2011. *"A data model to express the transport format of information about assets and the relationships between assets and reports."*

[24] From Waltermire, D., Halbardier, A., Humenansky, A., Mell, P. NIST Interagency Report (IR) 7800 (Draft), Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains. Maryland: National Institute of Standards and Technology; 2012. *Activities associated with understanding the relationship of assets across an enterprise.*

[25] From Waltermire, D., Halbardier, A., Humenansky, A., Mell, P. NIST Interagency Report (IR) 7800 (Draft), Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains. Maryland: National Institute of Standards and Technology; 2012. *Activities associated with verifying the status of configuration of computing devices across an enterprise.*

and vulnerability management[26]). This section is not intended to be a comprehensive review of all security automation standards and specifications, but instead will provide a high-level overview that furthers investigation.

Security Content Automation Protocol

The Security Content Automation Protocol (SCAP)[27] provides the bindings for supporting the layer 2 data domains through a series of specifications. SCAP provides a "suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans" [5] includes: languages (*XCCDF*,[28] *OVAL*®,[29] *OCIL*™[30]), reporting formats (*ARF*[31]), enumerations (*CPE*™,[32] *CCE*™,[33] and *CVE*™[34]), measurement and scoring systems (*CVSS*,[35] *CCSS*[36]), and supports the preservation of integrity (*TMSAF*)[37] of content and results. Table 12.2 provides a description of the five categories that cover the component specifications included within SCAP.

Cybersecurity Information Exchange Framework

Cybersecurity Information Exchange (CYBEX)[38] was produced by the International Telecommunication Union (ITU) Study Group (SG) 17.[39] CYBEX provides a model and technique for exchanging cybersecurity information (e.g., vulnerability and incident). It focuses on providing the means to support a trusted bi-directional exchange, but does not extend to the acquisition or use of the cybersecurity information which

[26] From Waltermire, D., Halbardier, A., Humenansky, A., Mell, P. NIST Interagency Report (IR) 7800 (Draft), Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains. Maryland: National Institute of Standards and Technology; 2012. *Activities associated with understanding the security posture through the identification of known vulnerabilities across an enterprise.*

[27] *Security Content Automation Protocol (SCAP)*. Available from: http://scap.nist.gov/index.html.

[28] *Extensible Configuration Checklist Description Format*. Available from: http://scap.nist.gov/specifications/xccdf/index.html.

[29] *Open Vulnerability and Assessment Language*. Available from: http://oval.mitre.org/.

[30] *Open Checklist Interactive Language*. Available from: http://scap.nist.gov/specifications/ocil/.

[31] *Asset Reporting Format*. Available from: http://scap.nist.gov/specifications/arf/.

[32] *Common Platform Enumeration*. Available from: http://scap.nist.gov/specifications/cpe/.

[33] *Common Configuration Enumeration*. Available from: http://cce.mitre.org/.

[34] *Common Vulnerabilities and Exposures.* Available from: http://cve.mitre.org/.

[35] *Common Vulnerability Scoring System*. Available from: http://www.first.org/cvss.

[36] *Common Configuration Scoring System.* Available from: http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf.

[37] *Trust Model for Security Automation Data*. Available from: http://scap.nist.gov/specifications/tmsad/.

[38] Recommendation X.1500, *Overview of cybersecurity information exchange*. Available from: http://www.itu.int/rec/T-REC-X.1500/en.

[39] *Cybersecurity Information Exchange techniques (CYBEX)*. Available from: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybex.aspx.

Table 12.2 SCAP Specification Categories [5]

Category	Description
Languages	Provide standard vocabularies and conventions for expressing security policy, technical check mechanisms, and assessment results
Reporting Formats	Provide the necessary constructs to express collected information in standardized formats
Enumerations	Define a standard nomenclature (naming format) and an official dictionary or list of items expressed using that nomenclature
Measurement and Scoring Systems	Evaluate specific characteristics of a security weakness (for example, software vulnerabilities and security configuration issues) and, based on those characteristics, generating a score that reflects their relative severity
Integrity	Helps to preserve the integrity of SCAP content and results

is contained within the organization's boundary. Although CYBEX is an international specification, it is briefly mentioned here as it relates to supporting the CAESARS FE where CM implementations within different organizational security boundaries are required to support the exchange of security-related information.

OPERATIONAL VISIBILITY AND CONTINUOUS MONITORING

The Federal Risk and Authorization Management Program (FedRAMP)'s ongoing assessment and authorization process includes a requirement for operational visibility and continuous monitoring requirements. In Figure 12.8, the CAESARS FE (discussed earlier in this chapter) is shown alongside the Cloud Security Alliance (CSA) Governance, Risk Management and Compliance (GRC) Stack.

The purpose of this diagram is to illustrate how the GRC Stack can support many of the aspects of the operational visibility and continuous monitoring requirements. In this section, the focus will be on providing an introduction to the components of the GRC Stack and a description of how they collectively can be used by Cloud Service Providers (CSPs), Third Party Assessment Organizations (3PAOs), and the federal government to achieve cost-effective compliance, and obtain security-related information to support CM activities.

Operational visibility focuses on demonstrating compliance on an ongoing basis through automated and manual processes. CSPs are required to provide data feeds (automated/manual), periodically assess security controls to determine continued effectiveness, and a report (annually) through a self-attestation certification. The data feeds should be in a compatible format that can be consumed by

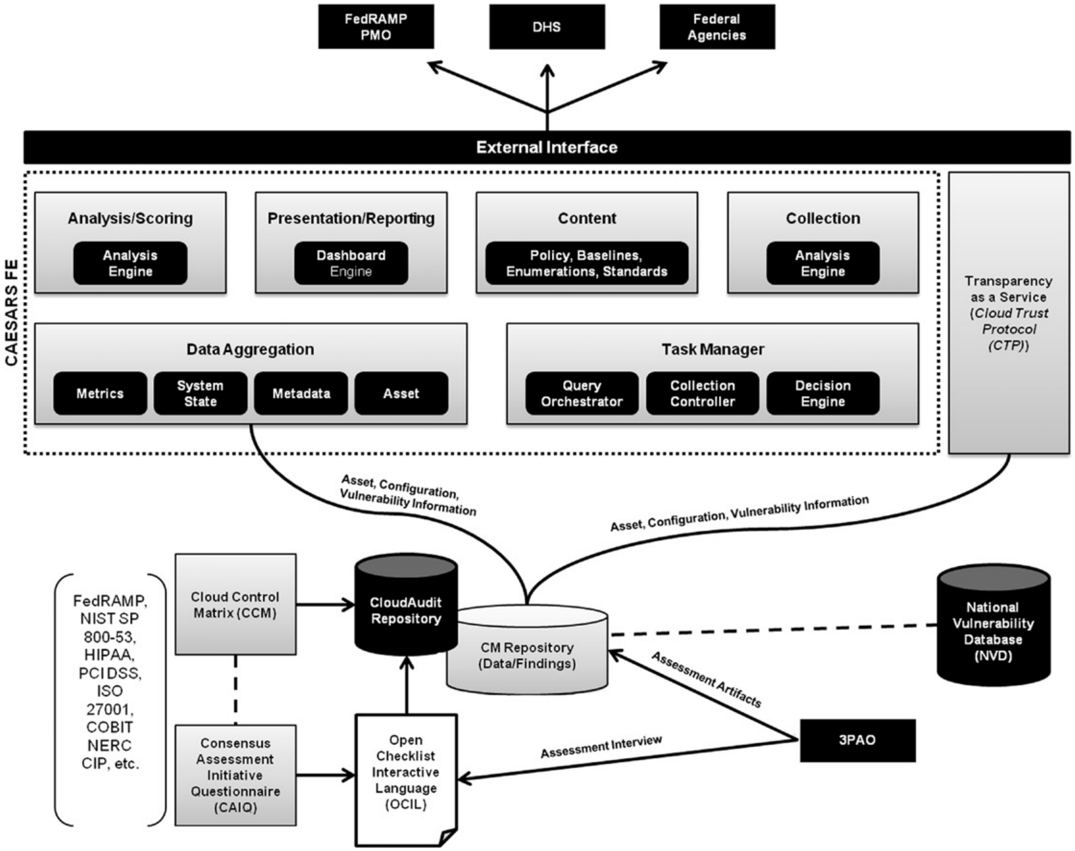

FedRAMP PMO
DHS
Federal Agencies
External Interface
CAESARS FE
Analysis/Scoring
Analysis Engine
Presentation/Reporting
Dashboard Engine
Content
Policy, Baselines, Enumerations, Standards
Collection
Analysis Engine
Data Aggregation
Metrics
System State
Metadata
Asset
Task Manager
Query Orchestrator
Collection Controller
Decision Engine
Transparency as a Service (Cloud Trust Protocol (CTP))
Asset, Configuration, Vulnerability Information
Asset, Configuration, Vulnerability Information
FedRAMP, NIST SP 800-53, HIPAA, PCI DSS, ISO 27001, COBIT NERC CIP, etc.
Cloud Control Matrix (CCM)
Consensus Assessment Initiative Questionnaire (CAIQ)
CloudAudit Repository
Open Checklist Interactive Language (OCIL)
CM Repository (Data/Findings)
National Vulnerability Database (NVD)
Assessment Artifacts
Assessment Interview
3PAO

FIGURE 12.8 Integrating Tools and Technologies into FedRAMP

the CyberScope.[40] CyberScope is an application that enables the federal government to support an "on-demand" view of the government-wide security posture. To enable the ability to achieve near-real-time risk management, the CyberScope application must handle manual and automated inputs from federal agencies based on data feeds produced using SCAP for FISMA reporting [6]. The annual assessment requires a 3PAO to conduct an assessment and the CSP's cloud service environment to certify the accuracy of the results before being submitted to the FedRAMP PMO and the leveraging federal agency to assist in integrating the cloud service into the enterprise-wide risk management process when making risk-based decisions.

The GRC Stack, depicted in Figure 12.8, comprises four components: *Cloud Control Matrix (CCM)*, *Consensus Assessment Initiative Questionnaire (CAIQ)*, *CloudAudit*, and *Cloud Trust Protocol (CTP)*. The CCM "is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider" [7]. The CCM provides a mapping between multiple compliance frameworks to include the FedRAMP security controls.[41] The CAIQ "provides a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider" [8]. The questions are aligned with the control requirements defined in the CCM. The next component is CloudAudit, which provides a common interface and namespace that enables streamlining the audit processes [9]. The last component, the CTP, is a mechanism by which consumers request for and receive information about the elements of transparency (EoT)[42] as applied to CSPs [10].

The data feeds focus on obtaining information to enable federal agencies to report on the level of performance of FISMA metrics[43] for asset management, configuration management, and vulnerability management. The CTP Elements of Transparency (EoTs) 3–4 (configuration information) and 5–7 (vulnerability information) focus on collecting and returning information, in a SCAP-consistent format, about the assets being used by the federal agency within the cloud service environment. Table 12.3 provides a description of EoTs 3–7:

The periodic assessment of security controls may be performed by a CSP to support other obligations of compliance or to support contractual requirements (or service-level agreements). The CCM, CAIQ, and CloudAudit collectively enable CSPs to perform internal assessment and third-party assessors (i.e., 3PAOs) to

[40] *CyberScope*. Available from: http://scap.nist.gov/use-case/cyberscope/.

[41] *FedRAMP Security Control Requirements*. Available from: http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip.

[42] From Cloud Trust Protocol (CTP) [Internet]. Washington, DC: Cloud Security Alliance; [cited 2012 June 22]. Available from: https://cloudsecurityalliance.org/research/ctp. *23 elements of information that provide characteristics of the compliance, security, privacy, integrity, and operational security.*

[43] *FY 2012 Chief Information Officer, Federal Information Security Management Act Reporting Metrics*. Available from: http://www.dhs.gov/xlibrary/assets/nppd/ciofismametricsfinal.pdf.

Table 12.3 Cloud Trust Protocol Configuration and Vulnerability EoTs [10]

EoT	Description
3	Current configuration
4	Differential comparison of current configuration and organizational policy
5	Results of last vulnerability assessment (scan)
6	Data of last vulnerability assessment (scan)
7	Request "on-demand" vulnerability assessment (scan)

obtain evidence of security control implementation and continued effectiveness. As illustrated in Figure 12.8, the CCM includes mappings to multiple frameworks that address those requirements defined by FedRAMP. The CAIQ can be converted into an OCIL-compliant automated checklist (questionnaire) that can be used to collect information through the assessment of security controls related to people and processes. This is specifically useful when assessing security controls that cannot be completely or fully monitored through security automation tools and technologies. CloudAudit provides a specification for a common namespace which aligns with the CCM to reduce the complexity of 3PAOs in collecting and storing evidentiary artifacts that support a CSPs' expression of its ability to meet compliance obligations.

SUMMARY

The use of security automation within information security programs focuses on achieving efficiency in the monitoring of security controls implemented within information systems. Automating CM activities requires understanding the processes that will be used by the organization, including the tools and technologies to provide a more frequent collection and analysis of security-related information. Therefore, the organization will need to ensure the CM strategy includes both a defined set of metrics and processes that will be used to monitor and respond to findings. Within FedRAMP the CSP's continuous monitoring capability supports the ongoing authorization and reauthorization decisions. Through the implementation of security automation, the CSP can more cost-effectively provide assurance of the security controls implemented and the confidence in their effectiveness. The CSA GRC Stack addresses many of the aspects of the operational visibility and continuous monitoring requirements of FedRAMP and supports federal agencies in reclaiming the transparency into the security posture of cloud services, enabling them to make more informed, risk-based decisions.

References

[1] Dempsey K, Nirali C, Johnson A, Johnston R, Jones A, Orebaugh A. NIST Special Publication (SP) 800-137, Information security continuous monitoring (ISCM) for federal information systems and organizations. Maryland: National Institute of Standards and Technology; 2011.

[2] Department of Homeland Security, Federal Network Security Branch. Continuous asset evaluation, situational awareness, and risk scoring (CAESARS) reference architecture report version 1.8. Washington: US Department of Homeland, Security; 2010.

[3] Mell P, Waltermire D, Feldman L, Booth H, Regland Z, Ouyang A, et al. NIST Interagency Report (IR) 7756 (Second Draft), CAESARS framework extension: an enterprise continuous monitoring technical reference model. Maryland: National Institute of Standards and Technology; 2012.

[4] Mell P, Waltermire D, Halbardier A, Feldman L. NIST Interagency Report (IR) 7799 (Draft), continuous monitoring reference model workflow, and specifications. Maryland: National Institute of Standards and Technology; 2012.

[5] Waltermire D, Quinn S, Sarfone K, Halbardier A. NIST Special Publication (SP) 800-126 Revision 2, The technical specification for the security content automation protocol (SCAP): SCAP version 1.2. Maryland: National Institute of Standards and Technology; 2011.

[6] CyberScope [Internet]. Maryland: National Institute of Standards and Technology [cited June 16, 2012]. <http://scap.nist.gov/use-case/cyberscope>.

[7] Cloud Control Matrix (CCM) [Internet]. Washington, DC: Cloud Security Alliance [cited June 22, 2012]. <https://cloudsecurityalliance.org/research/ccm>.

[8] Consensus Assessment Initiative [Internet]. Washington, DC: Cloud Security Alliance [cited June 22, 2012]. <https://cloudsecurityalliance.org/research/cai>.

[9] CloudAudit [Internet]. Washington, DC: Cloud Security Alliance [cited June 22, 2012]. <https://cloudsecurityalliance.org/research/cloudaudit>.

[10] Cloud Trust Protocol (CTP) [Internet]. Washington, DC: Cloud Security Alliance [cited June 22, 2012]. <https://cloudsecurityalliance.org/research/ctp>.

CHAPTER

A Case Study for Cloud Service Providers 13

INFORMATION IN THIS CHAPTER:

- Case Study Scenario: "Healthcare Exchange"
- Applying the Risk Management Framework within FedRAMP

CASE STUDY SCENARIO: "HEALTHCARE EXCHANGE"

The Patient Privacy and Protection Act,[1] recently signed into law, creates a new requirement for patient healthcare exchanges to be built, herein referred to as "Healthcare Exchange." The "Federal Agency" responsible for implementing the requirements of the law has chosen to use an operating expense model instead of a capital expense model, and usage-based pricing for processing, storage, bandwidth, and license management, and to support elasticity as demand for computing resources may change over time.

Since the "Federal Agency" will require collaboration with external partners to support the development of State "Healthcare Exchanges," the "Federal Agency" has chosen to acquire Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) environments from one provider to support the delivery of a computing platform and an application platform (similar to the cloud configuration use case included in Figure 13.1) where the States could build, test, deploy, and run portable, interoperable, and secure State "Healthcare Exchanges." This enables the "Federal Agency" to quickly meet its requirements under the new law. In addition, the IaaS/PaaS environments will be used by other federal agencies to support the development of a Federal "Healthcare Exchange" and other functions required to share information between State and federal government entities.

The cloud computing environment will also be used to support a "Federal Agency" mission and will contain federal information and information systems. Therefore, the infrastructure and platform environment of the cloud computing stack will be required to address federal cloud computing security standards. To reduce the complexity, the scenario will be limited to a discussion of only the Federal "Healthcare Exchange." The cloud computing infrastructure (IaaS/PaaS) will be required to address not only federal information security requirements under FedRAMP, but

[1] This Act is fictitious and does not exist.

Federal Cloud Computing. http://dx.doi.org/10.1016/B978-1-59-749737-4.00013-7

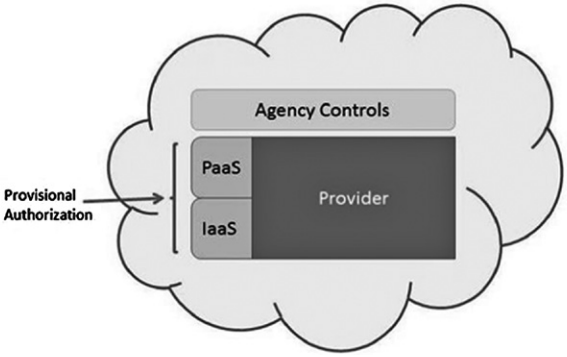


FIGURE 13.1 IaaS/PaaS Cloud Configuration Use Case [16]

also to meet all data management safeguard requirements required for the protection of Personally Identifiable Information (PII), Personal Health Information (PHI), and Federal Tax Information (FTI) data.

In this chapter, we will discuss the application of the FedRAMP deliverable documents to the FedRAMP Security Assessment Process Area included within Figure 13.2 under the Cloud Service Provider column. The case study in this section will be used to support the discussion.

APPLYING THE RISK MANAGEMENT FRAMEWORK WITHIN FEDRAMP

This section will focus on the application of Steps 1–5 of the NIST Risk Management Framework (RMF), which corresponds to Steps 1.1–1.3 of the Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Process Area. The case study provided in the last section will be used as a basis for illustrating how to approach using the FedRAMP deliverables to support a FedRAMP Provisional Authorization. Figure 13.3 provides the roadmap for the topics that will be presented.

Categorize Information System

The Cloud Service Provider (CSP) must identify the applicable information types and conduct a security categorization[2] of the cloud service to determine the impact level. As depicted in Figure 13.4, the CSP can use available federal governmental standards, guidelines, and regulations, and industry-specific "best practices" to assist in establishing a characterization of types of information currently stored, processed, or transmitted in the cloud service environment. The Federal Information Processing Standard (FIPS) 199 analysis represents the information type and sensitivity levels of the CSP's cloud service offering and is not intended to include sensitivity levels for federal

[2] Security categorization is discussed in detail in Chapter 5, Applying the Risk Management Framework.

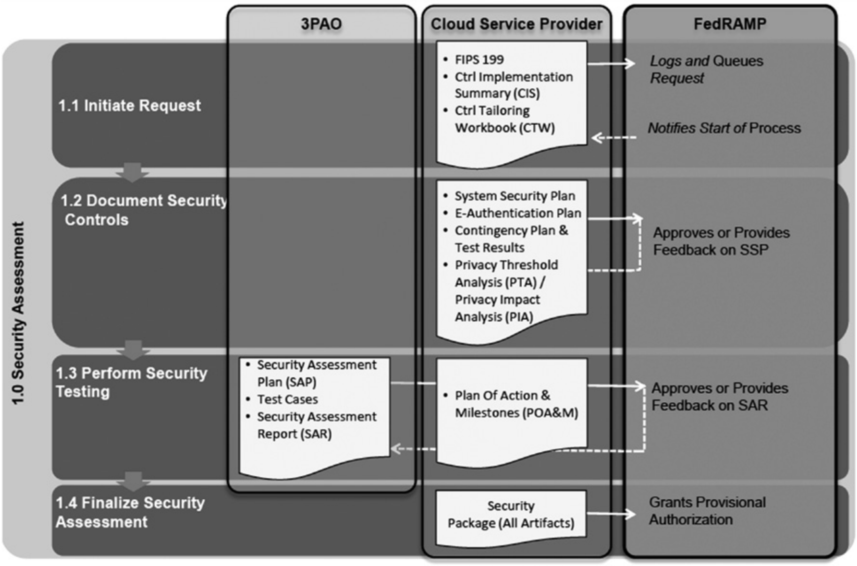
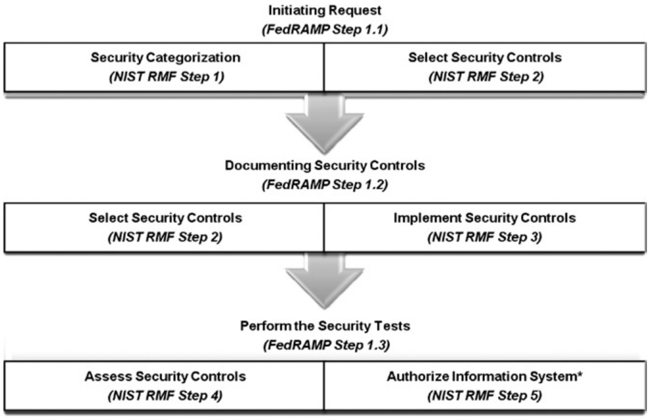

3PAO
Cloud Service Provider
FedRAMP
1.0 Security Assessment
1.1 Initiate Request
• FIPS 199
• Ctrl Implementation Summary (CIS)
• Ctrl Tailoring Workbook (CTW)
Logs and Queues Request
Notifies Start of Process
1.2 Document Security Controls
• System Security Plan
• E-Authentication Plan
• Contingency Plan & Test Results
• Privacy Threshold Analysis (PTA) / Privacy Impact Analysis (PIA)
Approves or Provides Feedback on SSP
1.3 Perform Security Testing
• Security Assessment Plan (SAP)
• Test Cases
• Security Assessment Report (SAR)
• Plan Of Action & Milestones (POA&M)
Approves or Provides Feedback on SAR
1.4 Finalize Security Assessment
Security Package (All Artifacts)
Grants Provisional Authorization

FIGURE 13.2 FedRAMP Security Assessment Process Area [1]



* NIST RMF Step 5, Task 5-1 requires preparing the plan of action and milestones based on the findings and recommendations of the security assessment report (developed in NIST RMF Step 4, Task 4-3).

FIGURE 13.3 Mapping between FedRAMP Security Assessment Processes Area and NIST RMF Steps

agency customer data, because they will be expected to perform a separate FIPS 199 analysis for federal information hosted on the CSP's cloud environment [15].

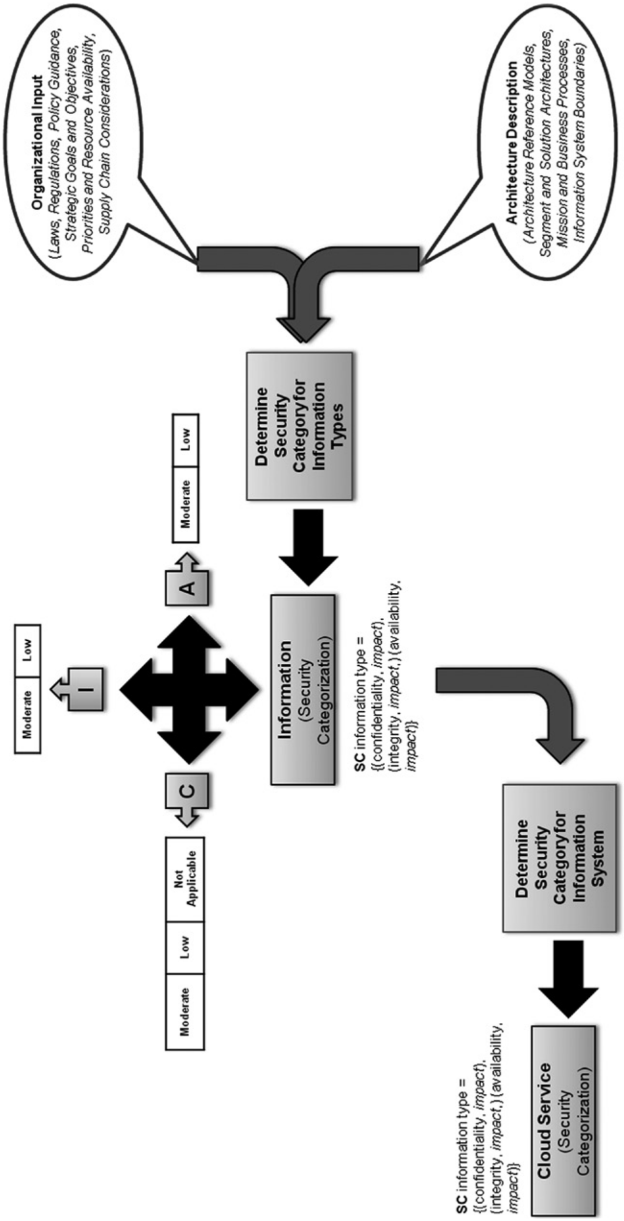

Organizational Input
(Laws, Regulations, Policy Guidance, Strategic Goals and Objectives, Priorities and Resource Availability, Supply Chain Considerations)
Architecture Description
(Architecture Reference Models, Segment and Solution Architectures, Mission and Business Processes, Information System Boundaries)
Determine Security Categoryfor Information Types
Information (Security Categorization)
SC information type = {(confidentiality, impact), (integrity, impact,) (availability, impact)}
C
Moderate
Low
Not Applicable
I
Moderate
Low
A
Moderate
Low
Determine Security Categoryfor Information System
C
Moderate
Low
I
Moderate
Low
A
Moderate
Low
Cloud Service (Security Categorization)
SC information type = {(confidentiality, impact), (integrity, impact,) (availability, impact)}

FIGURE 13.4 Role of Cloud Service Provider in the Security Categorization Process

Once the CSP has identified all the potential information types, the CSP will need to document this information in the FIPS 199.[3]

In documenting the FIPS 199, the CSP will need to provide an overview of the cloud service (i.e., high-level system description). Cloud services generally operate through the concept of a shared responsibility model, where both the CSP and the "Federal Agency" consumer will share the responsibility[4] for specific aspects of securing the cloud environment. Therefore the FIPS 199 completed by the CSP will need to address only[5] the information types and sensitivity levels of the cloud service for which the CSP is responsible. For example, Table 13.1 provides the information types that may be applicable to the IaaS and PaaS provider.

However, if the CSP operated a Software as a Service (SaaS) cloud service, all applicable information types will need to be examined. This may require the CSP to become familiar with the specific business use cases[6] and the types of information that the "Federal Agency" customer would process, store, or transmit in the cloud environment as a basis for determining the security categorization of the cloud service. This activity would be accomplished by using publicly available information from government-wide or agency-specific Federal Enterprise Architecture (FEA)[7] or Federal Segment Architecture (FSA) documentation.[8] A segment architecture is a "detailed results-oriented architecture (baseline and target) and a transition strategy for a portion or segment[9] of the enterprise" [3]. Tables 13.2–13.4 provide a list of potential information

[3] From FedRAMP Program Management Office (PMO). FedRAMP Template and Process Quick Guide. Washington: US General Services Administration; 2012. *"The Federal Information Processing Standard 199 (FIPS-199) Categorization (Security Categorization) report is a key document in the security authorization package developed for submission to the Federal Risk and Authorization Management Program (FedRAMP) authorizing officials. The FIPS-199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models (Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The ultimate goal of the security categorization is for the cloud service provider (CSP) to be able to select and implement the FedRAMP security controls applicable to its environment."*

[4] From FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) Version 1.1. Washington: US General Services Administration; 2012. *The Control Implementation Summary (CIS) document is used to enable the CSP to delineate where both the CSP and a federal agency may have a shared responsibility.*

[5] From FedRAMP Program Management Office (PMO). Guide to Understanding FedRAMP Version 1.1. Washington: US General Services Administration; 2012. *"Customer agencies will be performing a separate FIPS 199 analysis for their customer owned data hosted on the system."*

[6] NIST Cloud Computing Business Use Cases Working Group. Available from: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/BusinessUseCases.

[7] Federal Enterprise Architecture (FEA). Available from: http://www.whitehouse.gov/omb/e-gov/fea.

[8] Federal Segment Architecture Methodology (FSAM). Available from: www.cio.gov/documents/fsamv1.pdf.

[9] From Architecture and Infrastructure Committee. Federal Segment Architecture Methodology Version 1.0. Washington: CIO Council; 2008. *"A business service segment includes common or shared business services supporting the core mission areas."*

Table 13.1 IaaS and PaaS Information Types [2]

Information Type	Description
C.3.5.1 System Development Information Type	System Development supports all activities associated with the in-house design and development of software applications.
C.3.5.2 Lifecycle/ Change Management Information Type	Lifecycle/Change Management involves the processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures.
C.3.5.3 System Maintenance Information Type	System Maintenance supports all activities associated with the maintenance of in-house designed software applications.
C.3.5.4 IT Infrastructure Maintenance Information Type	IT Infrastructure Maintenance involves the planning, design, implementation, and maintenance of an IT infrastructure to effectively support automated needs (i.e., operating systems, applications software, platforms, networks, servers, printers, etc.). IT infrastructure maintenance also includes information systems configuration and security policy enforcement information. This information includes password files, network access rules and implementing files and/or switch setting, hardware and software configuration settings, and documentation that may affect access to the information system's data, programs, and/or processes.
C.3.5.5 Information Security Information Type	IT Security involves all functions pertaining to the securing of federal data and systems through the creation and definition of security policies, procedures, and controls covering such services as identification, authentication, and non-repudiation.
C.3.5.6 Record Retention Information Type	Records Retention involves the operations surrounding the management of the official documents and records for an agency.
C.3.5.7 Information Management Information Type	Information Management involves the coordination of information collection, storage, and dissemination, and destruction as well as managing the policies, guidelines, and standards regarding information management.
C.3.5.8 System and Network Monitoring Information Type	System and Network Monitoring supports all activities related to the real-time monitoring of systems and networks for optimal performance.
C.3.5.9 Information Sharing Information Type	The BRM provided in the *FEA Consolidated Reference Model Document, Version 2.3*, October 2007 specifies Information Sharing as relating to any method or function, for a given business area, facilitating: data being received in a usable medium by one or more departments or agencies as provided by a separate department or agency or other entity; and data being provided, disseminated, or otherwise made available or accessible by one department or agency for use by one or more separate departments or agencies, or other entities, as appropriate.

Table 13.2 Service Delivery Support Information Types [2] (*continued*)

Information Type	Confidentiality	Integrity	Availability
Controls and Oversight			
Corrective Action (Policy/Regulation)	Low	Low	Low
Program Evaluation	Low	Low	Low
Program Monitoring	Low	Low	Low
Regulatory Development			
Policy and Guidance Development	Low	Low	Low
Public Comment Tracking	Low	Low	Low
Regulatory Creation	Low	Low	Low
Rule Publication	Low	Low	Low
Planning and Budgeting			
Budget Formulation	Low	Low	Low
Capital Planning	Low	Low	Low
Enterprise Architecture	Low	Low	Low
Strategic Planning	Low	Low	Low
Budget Execution	Low	Low	Low
Workforce Planning	Low	Low	Low
Management Improvement	Low	Low	Low
Budgeting and Performance Integration	Low	Low	Low
Tax and Fiscal Policy	Low	Low	Low
Internal Risk Management and Mitigation			
Contingency Planning	Moderate	Moderate	Moderate
Continuity of Operations	Moderate	Moderate	Moderate
Service Recovery	Low	Low	Low
Revenue Collection			
Debt Collection	Moderate	Low	Low
User Fee Collection	Low	Low	Moderate
Federal Asset Sales	Low	Moderate	Low
Public Affairs			
Customer Services	Low	Low	Low
Official Information Dissemination	Low	Low	Low
Product Outreach	Low	Low	Low
Public Relations	Low	Low	Low
Legislative Relations			
Legislation Tracking	Low	Low	Low

Table 13.2 Service Delivery Support Information Types [2] (*continued*)

Information Type	Confidentiality	Integrity	Availability
Legislation Testimony	Low	Low	Low
Proposal Development	Moderate	Low	Low
Congressional Liaison Operations	Moderate	Low	Low
General Government			
Central Fiscal Operations	Moderate	Low	Low
Legislative Functions	Low	Low	Low
Executive Functions	Low	Low	Low
Central Property Management	Low	Low	Low
Central Personnel Management	Low	Low	Low
Taxation Management	Moderate	Low	Low
Central Records and Statistics Management	Moderate	Low	Low
Income Information	Moderate	Moderate	Moderate
Personal Identity and Authentication	Moderate	Moderate	Moderate
Entitlement Event Information	Moderate	Moderate	Moderate
Representative Payee Information	Moderate	Moderate	Moderate
General Information	Low	Low	Low

Table 13.3 Resource Management Information Types [2]

Information Type	Confidentiality	Integrity	Availability
Administrative Management			
Facilities, Fleet, and Equipment Mgmt	Low	Low	Low
Help Desk Services	Low	Low	Low
Security Management	Moderate	Moderate	Low
Travel	Low	Low	Low
Workplace Policy Development and Management	Low	Low	Low
Financial Management			
Asset and Liability Management	Low	Low	Low

Table 13.3 Resource Management Information Types [2] (*continued*)

Information Type	Confidentiality	Integrity	Availability
Reporting and Information	Low	Moderate	Low
Funds Control	Moderate	Moderate	Low
Accounting	Low	Moderate	Low
Payments	Low	Moderate	Low
Collections and Receivables	Low	Moderate	Low
Cost Accounting/ Performance Measurement	Low	Moderate	Low
Human Resource Management			
HR Strategy	Low	Low	Low
Staff Acquisition	Low	Low	Low
Organization and Position Management	Low	Low	Low
Compensation Management	Low	Low	Low
Benefits Management	Low	Low	Low
Employee Performance Management	Low	Low	Low
Employee Relations	Low	Low	Low
Labor Relations	Low	Low	Low
Separation Management	Low	Low	Low
Human Resources Development	Low	Low	Low
Supply Chain Management			
Goods Acquisition	Low	Low	Low
Inventory Control	Low	Low	Low
Logistics Management	Low	Low	Low
Services Acquisition	Low	Low	Low
Information and Technology Management			
System Development	Low	Moderate	Low
Lifecycle/Change Management	Low	Moderate	Low
System Maintenance	Low	Moderate	Low
IT Infrastructure Maintenance	Low	Low	Low
Information System Security	Low	Moderate	Low
Record Retention	Low	Low	Low
Information Management	Low	Moderate	Low
System and Network Monitoring	Moderate	Moderate	Low
Information Sharing	N/A	N/A	N/A

Table 13.4 Mission-Based Information Types [2]

Information Type	Confidentiality	Integrity	Availability
Defense and National Security	***Nat'l Security***	***Nat'l Security***	***Nat'l Security***
Homeland Security			
Border Control and Transportation Security	Moderate	Moderate	Moderate
Key Asset and Critical Infrastructure Protection	High	High	High
Catastrophic Defense	High	High	High
Executive Functions of the EOP	High	Moderate	High
Intelligence Operations	High	High	High
Disaster Management			
Disaster Monitoring and Prediction	Low	High	High
Disaster Preparedness and Planning	Low	Low	Low
Disaster Repair and Restoration	Low	Low	Low
Emergency Response	Low	High	High
International Affairs and Commerce			
Foreign Affairs	High	High	Moderate
International Development and Humanitarian Aid	Moderate	Low	Low
Global Trade	High	High	High
Natural Resources			
Water Resource Management	Low	Low	Low
Conservation, Marine, and Land Management	Low	Low	Low
Recreational Resource Management and Tourism	Low	Low	Low
Agricultural Innovation and Services	Low	Low	Low
Energy			
Energy Supply	Low	Moderate	Moderate
Energy Conservation and Preparedness	Low	Low	Low
Energy Resource Management	Moderate	Low	Low
Energy Production	Low	Low	Low
Environmental Management			
Environmental Monitoring/Forecasting	Low	Moderate	Low
Environmental Remediation	Moderate	Low	Low

Table 13.4 Mission-Based Information Types [2] (*continued*)

Information Type	**Confidentiality**	**Integrity**	**Availability**
Defense and National Security	***Nat'l Security***	***Nat'l Security***	***Nat'l Security***
Pollution Prevention and Control	Low	Low	Low
Economic Development			
Business and Industry Development	Low	Low	Low
Intellectual Property Protection	Low	Low	Low
Financial Sector Oversight	Moderate	Low	Low
Industry Sector Income Stabilization	Moderate	Low	Low
Community and Social Services			
Homeownership Promotion	Low	Low	Low
Community and Regional Development	Low	Low	Low
Social Services	Low	Low	Low
Postal Services	Low	Moderate	Moderate
Transportation			
Ground Transportation	Low	Low	Low
Water Transportation	Low	Low	Low
Air Transportation	Low	Low	Low
Space Operations	Low	High	High
Education			
Elementary, Secondary, and Vocational Education	Low	Low	Low
Higher Education	Low	Low	Low
Cultural and Historic Preservation	Low	Low	Low
Cultural and Historic Exhibition	Low	Low	Low
Workforce Management			
Training and Employment	Low	Low	Low
Labor Rights Management	Low	Low	Low
Worker Safety	Low	Low	Low
Health			
Access to Care	Low	Moderate	Low
Population Health Management and Consumer Safety	Low	Moderate	Low
Health Care Administration	Low	Moderate	Low
Health Care Delivery Services	Low	High	Low
Health Care Research and Practitioner Education	Low	Moderate	Low

Table 13.4 Mission-Based Information Types [2] (*continued*)

Information Type	Confidentiality	Integrity	Availability
Defense and National Security	***Nat'l Security***	***Nat'l Security***	***Nat'l Security***
Income Security			
General Retirement and Disability	Moderate	Moderate	Moderate
Unemployment Compensation	Low	Low	Low
Housing Assistance	Low	Low	Low
Food and Nutrition Assistance	Low	Low	Low
Survivor Compensation	Low	Low	Low
Law Enforcement			
Criminal Apprehension	Low	Low	Moderate
Criminal Investigation and Surveillance	Moderate	Moderate	Moderate
Citizen Protection	Moderate	Moderate	Moderate
Leadership Protection	Moderate	Low	Low
Property Protection	Low	Low	Low
Substance Control	Moderate	Moderate	Moderate
Crime Prevention	Low	Low	Low
Trade Law Enforcement	Moderate	Moderate	Moderate
Litigation and Judicial Activities			
Judicial Hearings	Moderate	Low	Low
Legal Defense	Moderate	High	Low
Legal Investigation	Moderate	Moderate	Moderate
Legal Prosecution and Litigation	Low	Moderate	Low
Resolution Facilitation	Moderate	Low	Low
Federal Correctional Activities			
Criminal Incarceration	Low	Moderate	Low
Criminal Rehabilitation	Low	Low	Low
General Science and Innovation			
Scientific and Technological Research and Innovation	Low	Moderate	Low
Space Exploration and Innovation	Low	Moderate	Low
Knowledge Creation and Management			
Research and Development	Low	Moderate	Low

Table 13.4 Mission-Based Information Types [2] (*continued*)

Information Type	Confidentiality	Integrity	Availability
Defense and National Security	***Nat'l Security***	***Nat'l Security***	***Nat'l Security***
General Purpose Data and Statistics	Low	Low	Low
Advising and Consulting	Low	Low	Low
Knowledge Dissemination	Low	Low	Low
Regulatory Compliance and Enforcement			
Inspections and Auditing	Moderate	Moderate	Low
Standards Setting/ Reporting Guideline Development	Low	Low	Low
Permits and Licensing	Low	Low	Low
Public Goods Creation and Management			
Manufacturing	Low	Low	Low
Construction	Low	Low	Low
Public Resources, Facility, and Infrastructure Management	Low	Low	Low
Information Infrastructure Management	Low	Low	Low
Federal Financial Assistance			
Federal Grants (Non-State)	Low	Low	Low
Direct Transfers to Individuals	Low	Low	Low
Subsidies	Low	Low	Low
Tax Credits	Moderate	Low	Low
Credits and Insurance			
Direct Loans	Low	Low	Low
Loan Guarantees	Low	Low	Low
General Insurance	Low	Low	Low
Transfers to State/Local Governments			
Formula Grants	Low	Low	Low
Project/Competitive Grants	Low	Low	Low
Earmarked Grants	Low	Low	Low
State Loans	Low	Low	Low
Direct Services for Citizens			
Military Operations	N/A	N/A	N/A
Civilian Operations	N/A	N/A	N/A

TIP

If the CSP determines, through a review of the recommended impact levels, that there are differences in the selected impact levels, the CSP will need to provide justification (rationale) for any changes. During the review, the following factors [5] can be used to assist the CSP in determining if the impact levels should be adjusted based on the applicable security objectives:

- Sensitivity of change of information when aggregated.
- Compromise in critical system functionality.
- Elevation based on extenuating circumstances.
- Integrity of public information, loss of system availability, privacy information, etc.

types and the recommended (provisional[10]) impact levels for the confidentiality, integrity, and availability security objective of *Low, Moderate,* or *High.*[11]

In addition, the CSP will need to ensure the "Federal Agency" customer using the cloud service collects, processes, or stores information types that do not exceed the high-water mark of low- or moderate-impact level for the confidentiality, integrity, and availability security objectives [4].

The role of the "Federal Agency" in the security categorization process is the characterization of the information that it plans to store, process, or transmit in the cloud service. The application of the security categorization process by the "Federal Agency" will require an evaluation of multiple sources of information,[12] to include, but not limited to, the organizational input from key stakeholders (e.g., other federal agencies and State partners), the architectural descriptions of the "Healthcare Exchange," and EA reference models used to establish a business case[13] as the basis for determining the security objectives for the types of information that will be processed, transmitted, or stored in the cloud service.

[10] From Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick J. NIST Special Publication (SP) 800-60 Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Maryland: National Institute of Standards and Technology; 2008. *"Provisional security impact levels are the initial or conditional impact determinations made until all considerations are fully reviewed, analyzed, and accepted in the subsequent categorization steps by appropriate officials."*

[11] Note, FedRAMP does not currently address "high-impact" sensitivity levels.

[12] It is important to understand that not all information might be available, however, since the security categorization effects the other steps of the NIST RMF, a regular review may be required to identify any changes that would have impact.

[13] From Office of Management and Budget (OMB). FY13 Guidance on Exhibit 300—Planning, Budgeting, Acquisition, and Management of IT Capital Assets. Washington: Executive Office of the President, Office of Management and Budget; 2011. *"The business case must demonstrate the relationship between the investment and the business, performance, data, services, application and technology layers of the agency's EA."*

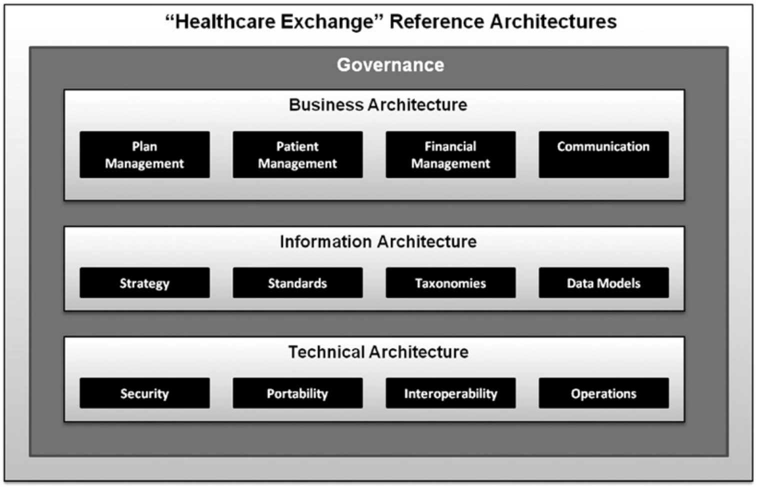


FIGURE 13.5 Exchange Reference Architecture Framework

The "Federal Agency" established a business case[14] for the "Healthcare Exchange" IT Investment. The "Healthcare Exchange" provides a platform for organizing health information. The "Federal Agency" identified two mission-essential functions supported by the IT Investment Exchange Systems and Data Services. Through an evaluation of the architectural descriptions (e.g., architecture reference models, mission, and business processes, etc.) and organizational inputs (laws, directives, policy guidance, etc.), specific mission-based information[15] and management and support information[16] can be identified and categorized using information associated with the "Healthcare Exchange" as a point of reference to understand the potential impact due to a compromise in the confidentiality (C), integrity (I), and availability (A).

The "Federal Agency" established Exchange Reference Architecture,[17] as illustrated in Figure 13.5, defines the key business information and technical areas and

[14] A business case assists stakeholders in making decisions regarding the viability of a proposed project effort. The Office of Management and Budget (OMB) requires a business case as part of Part 7, Section 300. Additionally, business cases are considered standard practice throughout private and public industry in addition to specific laws and regulations that mandate business cases for certain project types.

[15] Information that is specific to individual departments and agencies or sets of departments and agencies.

[16] Information that supports the delivery of services or the management of resources.

[17] From Office of Management and Budget (OMB). The Common Approach to Federal Enterprise Architecture. Washington: Executive Office of the President, Office of Management and Budget; 2012. *"A 'Reference Architecture' is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions."*

Table 13.5 Key Data Definitions

Term	Definition
PII	As defined in OMB Memorandum M-07-16, PII refers to any "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." [7]
PHI	The HIPAA Privacy Rule defines PHI as individually identifiable health information that is held or transmitted in any form or medium by a covered entity [8]
IIHI	HIPAA defines IIHI as any information, including demographic information, collected from an individual that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and identifies the individual or where there is a reasonable basis to believe that the information can be used to identify the individual [9]
FTI	Federal Tax Returns and return information are confidential, as required by IRC Section 6103. The IRS uses the IRC to ensure that agencies, bodies, and commissions maintain appropriate safeguards to protect the information confidentiality [10]

also provides a high-level view of the Business Architecture (BRM),[18] Information Architecture (DRM),[19] and Technical Reference Architecture (TRM).[20] The Exchange References Architecture[21] provides the description of the core business areas and processes in the Business Architecture that will be used to exchange information defined in the Information Architecture and supported through the implementation of the business and information requirements in the Technical Reference Architecture.

The "Federal Agency" also identified key data types in Table 13.5 to use as a basis for characterizing the types of information that will require the highest level of

[18] From Office of Management and Budget (OMB). FY2014 Guide on Exhibit 53 and 300—Information Technology and E-Government. Washington: Executive Office of the President, Office of Management and Budget; 2012. *"Business Reference Model (BRM) a classification taxonomy used to describe mission sectors, business functions, and services that are performed within and between Federal agencies and with external partners."*

[19] From Office of Management and Budget (OMB).Consolidated Reference Model Version 2.3. Washington: Executive Office of the President, Office of Management and Budget; 2007. *Data Reference Model is "a flexible and standards-based framework to enable information sharing and reuse across the federal government via the standard description and discovery of common data and the promotion of uniform data management practices."*

[20] From Office of Management and Budget (OMB). Consolidated Reference Model Version 2.3. Washington: Executive Office of the President, Office of Management and Budget; 2007. *Technical Reference Model (TRM) is a "technical framework categorizing the standards and technologies to support and enable the delivery of Service Components and capabilities."*

[21] Similar to the role of the enterprise architecture discussed in detail in Chapter 5, Applying the NIST Risk Management Framework.

TIP

Depending on which cloud service model (IaaS, PaaS, SaaS) and deployment model (public, hybrid, private, community) is chosen as part of the implementation, the cloud service may become part of or completely (in circumstances where the entire business and mission function is outsourced) integrated into federal agencies' enterprise architecture (EA). This dependence by federal agencies can introduce many challenges when applying the RMF to cloud services.

The *Federal Cloud Computing Strategy* highlighted, as part of the "Decision Framework for Cloud Migration," the need for federal agencies to provision cloud services by integrating them into their wider application portfolio. This will require federal agencies to evaluate architectural compatibility of the cloud services and other critical applications [6]. EA, as a tool, provides federal agencies with a structured approach for ensuring the interoperability, portability, and security of cloud computing adoption through coordination with the federal government EA programs. EA can also assist in determining the requirements for addressing governance, risk management, and compliance (GRC) (see Figure 13.4).

protection when conducting security categorization. In addition, a list of related laws, standards, guidelines, and organizational agreements for consideration was developed and mapped against the "Healthcare Exchange" participants as organizational inputs into the security categorization process.

Based on the case study used in this section, several potential information types may be selected by the "Federal Agency" such as:

- $SC_{\text{Access to Care Information Type}}$[22] = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}.
- $SC_{\text{Health Care Delivery Services Information Type}}$[23] = {(confidentiality, Low), (integrity, High), (availability, Low)}.
- $SC_{\text{Taxation Management Information Type}}$[24] = {(confidentiality, Moderate), (integrity, Low), (availability, Low)}.

[22] From Stine, K., Kissel, R., Barker, W., Lee, A., Fahlsing, J. NIST Special Publication (SP) 800-60 Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. Maryland: National Institute of Standards and Technology; 2008. *This information includes streamlining efforts to receive care; ensuring care is appropriate in terms of type, care, intensity, location and availability; providing seamless access to health knowledge, enrolling providers; performing eligibility determination, and managing patient movement.*

[23] From Stine, K., Kissel, R., Barker, W., Lee, A., Fahlsing, J. NIST Special Publication (SP) 800-60 Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. Maryland: National Institute of Standards and Technology; 2008. *This information includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation.*

[24] From Stine, K., Kissel, R., Barker, W., Lee, A., Fahlsing, J. NIST Special Publication (SP) 800-60 Revision 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. Maryland: National Institute of Standards and Technology; 2008. *This information includes activities associated with the implementation of the Internal Revenue Code and the collection of taxes in the United States and abroad.*

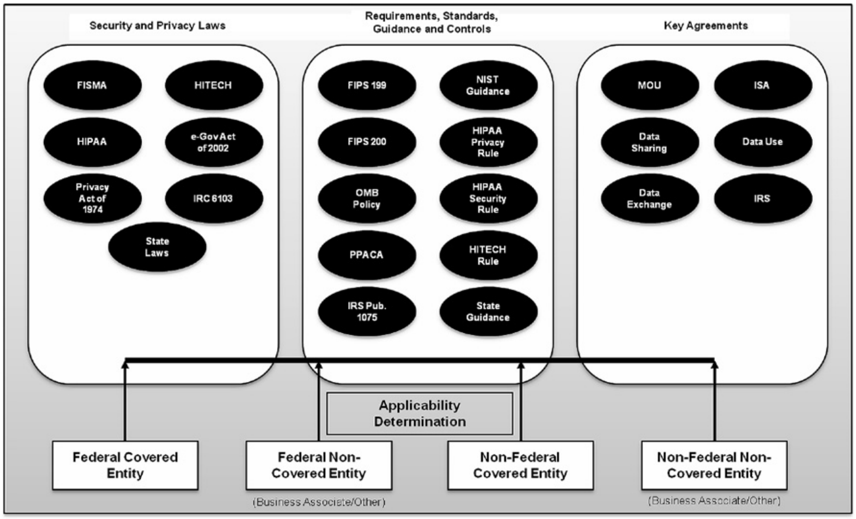


FIGURE 13.6 Laws, Required Standards, and Guidance

Select Security Controls

The security control selection process relies on the definition of the security control boundary and a clear delineation of the security controls responsibility across service and deployment models. It also requires an understanding of any decomposition of cloud services into associated subsystems and the mapping of data flows to ensure adequate protective measures are applied cost-effectively to sensitive data throughout the cloud service lifecycle.

The implementation of the "Healthcare Exchange" includes a complicated set of security and privacy requirements. Figure 13.6 illustrates the different requirements derived from various laws, requirements, standards, guidelines, and control frameworks, in addition to any organization-specific requirements established by the information-sharing agreement.[25] For example, under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rule, covered entities "must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information" [11]. These requirements could include the additional

[25] From Grance, T., Hash, J., Peck, S., Smith, J., Korow-Diks, K. NIST Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems. Maryland: National Institute of Standards and Technology; 2002. *"Organizations should examine privacy issues related to data that will be exchanged or passed over the interconnection and determine whether such use is restricted under current statutes, regulations, or policies."*

administrative, physical, and technical safeguards that exceed the security control requirements defined in the FedRAMP baseline security controls.[26]

Defining the Boundary

The first step in the security control selection process is to define the boundary.[27] This provides the scope of protection for the system components and interfaces for interconnections and is critical for understanding and clarifying the shared responsibilities for implementing, monitoring, and assessing security controls allocated[28] across the various cloud service and deployment models. Although only conceptual, Figure 13.7 provides a high-level illustration of the factors that might be considered when allocating security controls and assigning ownership between the CSP and the "Federal Agency." For example, identifying those controls which are inherited from one or more organizations (*common controls*) or are shared between one or more organizations (*hybrid controls*), requires establishing roles and responsibilities based on the different deployment models and service models.

In addition, establishing a definition of both the authorization boundary and the level of control of the resources can help clarify the delineation of the specific aspects being inherited. For security control allocation to be successful, in most cases it requires building trusted relationships based on the sharing of evidence that specific security controls are implemented, including any assessment results (or a summary) and information collected as part of an ongoing continuous monitoring program. The Control Implementation Summary (CIS)[29] will be used by the CSP to indicate who owns the responsibility (or the shared responsibility) to implement and manage the controls, and the implementation status of the controls [12].

In this scenario the CSP provides the implementation status (i.e., in-place, partially implemented, planned, alternative implementation, and not applicable) for security control implementations that relates to the infrastructure and the platform,

[26] NIST Special Publication (SP) 800-66 Revision 1, *Introductory Resource Guide for Implementing the HIPAA Security Rule,* discusses security considerations and resources for use when implementing the requirements of the Security Rule.

[27] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Well-defined boundaries establish the scope of protection for organizational information systems (i.e. what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes."*

[28] From Joint Task Force Transformation Initiative, NIST Special Publication (SP) 800-53 Revision 3, Recommended Security Controls for Federal Information System and Organizations. Maryland: National Institute of Standards and Technology; 2010. *"Allocation is a term used to describe the process an organization employs: (i) to determine whether security controls are defined as system-specific, hybrid, or common; and (ii) to assign security controls to specific information system components responsible for providing a particular security capability (e.g. router, server, remote sensor)."*

[29] From FedRAMP Program Management Office (PMO). FedRAMP FIPS 199 Categorization Template. Washington: US General Services Administration; 2012. *"The CIS report includes control implementation responsibility and implementation status of the FedRAMP security controls."*

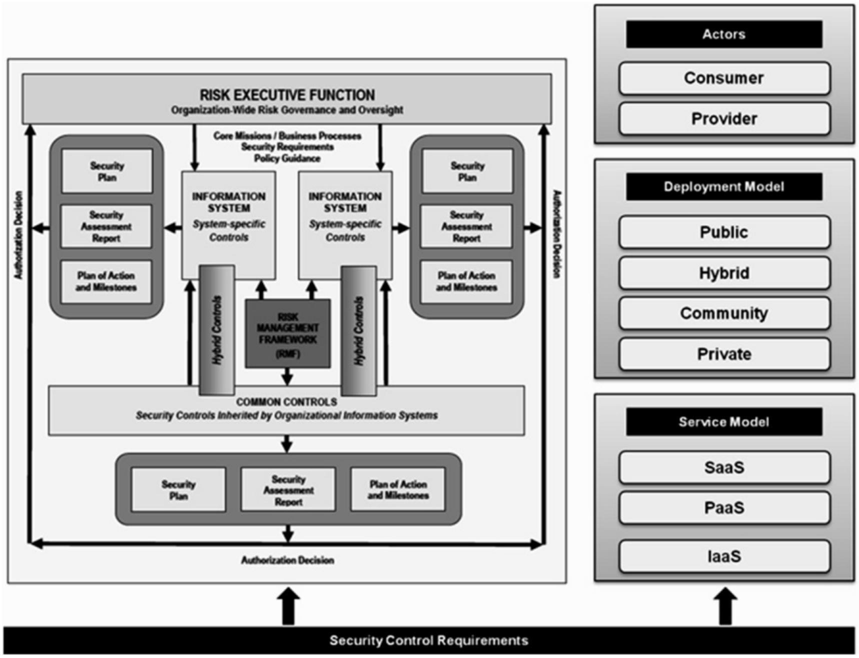


FIGURE 13.7 Security Control Allocation

and indicates where the security control originates (i.e., service provider corporate network, service provider cloud service-specific, shared between the cloud service and the corporate network, configured by the customer, customer-specific hardware/software, and shared management between the service provider and the customer).

Tailoring and Supplementing

The security controls selection process uses the security categorization to determine the appropriate initial baseline of security controls (i.e., Low or Moderate) that will provide adequate protection for the information and information systems that reside within the cloud service environment. A cloud service may require the implementation of alternative or compensating security controls not included in the initial baseline, or adding additional security controls or enhancements to address unique organizational needs based on a risk assessment or organization-specific security requirement. For this purpose, the Control Tailoring Workbook (CTW) provides the CSP with a listing of the FedRAMP security controls applicable for the cloud environment and assists in identifying the exception scenarios for the service offering so that the platform can be pre-qualified before resources are used to develop all of the other requisite FedRAMP documentation requirements [12].

Implement and Document Security Controls

Documenting security controls within the cloud service requires the CSP to describe how the security controls were implemented in the System Security Plan (SSP). In the previous section, security controls were allocated based on specific responsibilities (i.e., inherited by another organization, shared between organizations, or implemented by an organization). In the SSP, information system components will need to be described based on the authorization boundary. The SSP details how the implementations address each required security control and enhancement in the selected, tailored, and supplemented security control baseline, descriptions of roles and responsibilities, and expected behavior of individuals with system access [12].

In addition, some security controls may require developing support documentation. For example, Table 13.6 identifies some of the documents that would be implemented by the CSP for FedRAMP.

Assessing Security Controls

The assessment of security controls is primarily driven by the security control assessor. Within FedRAMP, an accredited third party assessment organization (3PAO) performs and independently tests the CSP's cloud service to determine the effectiveness of security control implementation [14]. A discussion of the 3PAO's responsibilities is beyond the scope of this section. Instead this section focuses on the Plan of Action and Milestones (POA&Ms).[30] Once the 3PAO has completed conducting an assessment of the security controls, the Security Assessment Report (SAR)[31] is developed, which is used by the CSP as a source for identifying, documenting, and managing the mitigation[32] of "medium"[33] and "high"[34] risk security vulnerabilities.[35] The POA&M is a tool used by the CSP, FedRAMP, and the "Federal Agency" when tracking and reporting on the progress of remediating security weaknesses and deficiencies. The POA&M[36] addresses the specific tasks and resources, including a schedule for completing the remediation activities.

[30] Office of Management and Budget (OMB) Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, preparing the plan of action and milestones (POA&Ms). Available from: http://www.whitehouse.gov/omb/memoranda_m02-01.

[31] From FedRAMP Program Management Office (PMO). Plan of Action and Milestones (Template). Washington: US General Services Administration; 2012. *POA&Ms are based on the findings and recommendations of the SAR excluding any remediation actions taken.*

[32] FedRAMP specifies 90 days for "medium" and 30 days for "high."

[33] Vulnerabilities are labeled "medium" if they have a CVSS base score of 4.0–6.9.

[34] Vulnerabilities are labeled "high" if they have a CVSS base score of 7.0–10.0.

[35] The Common Vulnerability Scoring System (CVSS) standard provides guidance on scoring vulnerabilities. Available from: http://www.first.org/cvss/cvss-guide.html.

[36] The POA&M document is one of three key documents (*SSP, SAR, and POA&M*) used by the JAB to make a determination of a provisional authorization and the federal agency in making a determination for leveraging the cloud service.

Table 13.6 SSP Supporting Documents [13]

Document Name	Security Control Requirement
IT Contingency Plan[a] (including Business Impact Analysis[b])	*CP-2—Contingency Plan* The organization: **a.** Develops a contingency plan for the information system that: – Identifies essential missions and business functions and associated contingency requirements; – Provides recovery objectives, restoration priorities, and metrics003B – Addresses contingency roles, responsibilities, assigned individuals with contact information; – Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; – Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and – Is reviewed and approved by designated officials within the organization; **b.** Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; **c.** Coordinates contingency planning activities with incident handling activities; **d.** Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*].
Configuration Management Plan[c]	*CM-9—Configuration Management Plan* The organization develops, documents, and implements a configuration management plan for the information system that: **a.** Addresses roles, responsibilities, and configuration management processes and procedures; **b.** Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and **c.** Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Table 13.6 SSP Supporting Documents [13] (*continued*)

Document Name	Security Control Requirement
Incident Response Plan[d]	*IR-9—Incident Response Plan* The organization: **a.** Develops an incident response plan that: – Provides the organization with a roadmap for implementing its incident response capability; – Describes the structure and organization of the incident response capability; – Provides a high-level approach for how the incident response capability fits into the overall organization; – Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; – Defines reportable incidents; – Provides metrics for measuring the incident response capability within the organization; – Defines the resources and management support needed to effectively maintain and mature an incident response capability; and – Is reviewed and approved by designated officials within the organization; **b.** Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; **c.** Reviews the incident response plan [*Assignment: organization-defined frequency*]; **d.** Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and **e.** Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].

Table 13.6 SSP Supporting Documents [13] (*continued*)

Document Name	Security Control Requirement
E-Authentication[e]	*IA-2—Identification and Authentication (Organizational Users)* The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). *IA-8—Identification and Authentication (Non-Organizational Users)* The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
Privacy Threshold Analysis and Privacy Impact Assessment[f]	*PL-5—Privacy Impact Assessment* The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

[a] *NIST Special Publication (SP) 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems contains sample Information System Contingency Plans for Low-Impact (A.1) and Moderate-Impact (A.2) systems. Available from: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.*

[b] *NIST Special Publication (SP) 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems contains sample Business Impact Analysis Template (Appendix B). Available from: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.*

[c] *NIST Special Publication (SP) 800-128, Guide for Security-Focused Configuration Management of Information Systems contains sample outline for a Security Configuration Management Plan (Appendix D). Available from: http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf.*

[d] *NIST Special Publication (SP) 800-61 Revision 2, Computer Security Incident Handling Guide contains a description of elements of the Incident Response Plan (Section 2.3.2—Plan Elements). Available from: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.*

[e] *NIST Special Publication (SP) 800-63-1, Electronic Authentication Guide contains information on e-authentication. Available from: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf. Additional information can be found at IDManagement.gov.*

[f] *Office of Management and Budget (OMB) Memorandum 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 provides guidance on conducting a privacy impact assessment (PIA). Available from: http://www.whitehouse.gov/omb/memoranda_m03-22.*

SUMMARY

This chapter presented a short case study to illustrate how the NIST RMF can be applied within the context of FedRAMP. In addition, some of the various FedRAMP deliverables were discussed as they relate to the security categorization, security control selection, and the implementation of the security controls (including supporting documentation) and documenting corrective actions resulting from the security controls assessment. Since the NIST RMF is a continuous process, documents will require regular reviews and updates on a continuous basis to address changes to the cloud service information system and the operating environment.

References

[1] FedRAMP Program Management Office (PMO). FedRAMP template and process quick guide. Washington: US General Services Administration; 2012.

[2] Stine K, Kissel R, Barker W, Lee A, Fahlsing J. NIST Special Publication (SP) 800-60 Revision 1, Volume II: Guide for mapping types of information and information systems to security categories. Maryland: National Institute of Standards and Technology; 2008.

[3] Architecture and Infrastructure Committee. Federal segment architecture methodology version 10. Washington: CIO Council; 2008.

[4] FedRAMP Program Management Office (PMO). FIPS 199 Categorization (Template). Washington: US General Services Administration; 2012.

[5] Stine K, Kissel R, Barker W, Fahlsing J, Gulick J. NIST Special Publication (SP) 800-60 Revision 1, Volume I: Guide for mapping types of information and information systems to security categories. Maryland: National Institute of Standards and Technology; 2008.

[6] Kundra V. Federal cloud computing strategy. Washington: Executive Office of the President, Office of Management and Budget; 2011.

[7] Johnson C. Office of Management and Budget (OMB) memorandum 07-16, safeguarding against and responding to the breach of personally identifiable information. Washington: Executive Office of the President, Office of Management and Budget; 2007.

[8] HIPAA Privacy Rule [Internet]. Washington: US Government printing office [cited June 18, 2012]. <http://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec160-103.pdf>.

[9] Health Insurance Portability and Accountability Act of 1996 [Internet]. Washington: US Government printing office [cited December 15, 2011]. <http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm>.

[10] IRC Section 6103, Confidentiality and disclosure of returns and return information [Internet]. Washington: US Government printing office [cited December 17, 2011]. <http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm>.

[11] For Covered Entities [Internet]. Washington: US Department of Health & Human Services [cited December 15, 2011]. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html>.

[12] FedRAMP Program Management Office (PMO). Guide to understanding FedRAMP version 1.1. Washington: US General Services Administration; 2012.

[13] Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53 Revision 3, Recommended security controls for federal information system and organizations. Maryland: National Institute of Standards and Technology; 2010.

[14] FedRAMP Program Management Office (PMO). FedRAMP Concept of Operations (CONOPS) version 1.0. Washington: US General Services Administration; 2012.

[15] FedRAMP Program Management Office (PMO). FedRAMP FIPS 199 Categorization Template. Washington: US General Services Administration; 2012.

[16] FedRAMP Program Management Office (PMO). Guide to Understanding FedRAMP. Washington: US General Services Administration; 2012.

Index

Note: Page numbers followed by "f" and "t" indicate figure and table respectively

This page is intentionally left blank