# TABLE OF CONTENTS



# TABLE OF FIGURES

[redacted]

# LIST OF TABLES

# 8 BSS RISK MANAGEMENT FRAMEWORK PLAN [L.30.2.7; G.5.6; NIST SP 800-37]

As a leading provider of telecommunications services to the U.S. Government, Verizon has an established, proven record in information security risk management utilizing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-series guidelines including, but not limited to *SP 800-37 Rev 1., Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. [redacted]

Verizon has worked closely with these government agencies to implement the processes identified in the NIST Risk Management Framework (RMF). Verizon's significant experience in this area has provided Verizon with a solid understanding of the NIST RMF and agency-specific information security and Assessment and Authorization (A&A) requirements. [redacted]

[redacted]

## 8.1 Purpose and Scope

This Business Systems Solution (BSS) RMF Plan describes Verizon's overarching approach to managing applicable risks to information systems and their contents as well as the steps that Verizon will take to integrate security requirements throughout the BSS System Development Life Cycle (SDLC) and to obtain and maintain an ATO from the GSA Authorizing Official (AO). This RMF Plan provides the following information:

- [redacted]

## 8.2 Applicable Standards and Guidelines

In providing EIS services, Verizon will comply with government identified federal and agency-specific IT security directives, standards, policies, and reporting requirements, as specified in the respective Task Order (TO). Where applicable, Verizon will comply with FISMA, Department of Defense (DoD), Intelligence Community and agency guidance and directives, including applicable Federal Information Processing Standards (FIPS), NIST SP 800-series guidelines, required government policies, and other applicable laws and regulations for protection and security of government IT.

**Table 8.2-1** lists key information security management standards and guidelines Verizon bases its approach to security references in support of the BSS RMF. When discussed in this RMF Plan, the versions of the documents identified in Table 8.2-1 are the applicable reference.

**Table 8.2-1. Applicable BSS RMF Documents.**

| Risk Management Framework Plan Applicable Documents |
|---|
| ▪ Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C, Section 301. Information Security). |
| ▪ Federal Information Security Modernization Act of 2014 (to amend Chapter 35 of 44 U.S.C.). |
| ▪ Clinger-Cohen Act of 1996 (Formerly known as the Information Technology Management Reform Act of 1996). |
| ▪ Privacy Act of 1974 (5 U.S.C. § 552a). |
| ▪ Homeland Security Presidential Directive 12 (HSPD-12), Policy for Identification for Federal Employees and Contractors, August 27, 2004. |
| ▪ E-Government Act of 2002 (Public Law 107-347). |
| ▪ Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004. |
| ▪ Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information System, March 2006. |
| ▪ Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, May 2001. |
| ▪ OMB Circular A-130, Management of Federal Information Resources (and Appendix III, Security of Federal Automated Information Resources, Transmittal Memorandum, No. 4, November 28, 2008. |
| ▪ OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003. |
| ▪ OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005. |
| ▪ OMB Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011. |
| ▪ OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, November 18, 2013. |
| ▪ OMB Memorandum M-15-01, Guidance on Improving Federal Information Security and Privacy Management Practices, October 3, 2014. |
| ▪ NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006. |
| ▪ NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments. September 2012. |
| ▪ NIST SP 800-34, Revision 1, Contingency Planning Guide for Information Technology Systems. May 2010. |
| ▪ NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010. |
| ▪ NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011. |
| ▪ NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy, September 2009. |
| ▪ NIST SP 800-47, Security Guide for Interconnecting Information Technology System, August 2002. |
| ▪ NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013. |
| ▪ NIST SP 800-53A, Revision 4, Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans, December 2014. |
| ▪ NIST SP 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008. |
| ▪ NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide, August 2012. |
| ▪ NIST SP 800-70 Revision 3, Agency & Center for Internet Security (CIS) Hardening Guides. |
| ▪ NIST SP 800-88 Revision 1, Guidelines for Media Sanitization, December 2014. |
| ▪ NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011. |
| ▪ NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, September 2011. |
| ▪ NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011. |
| ▪ NIST SP 800-171, Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations, June 2015. |
| ▪ GSA CIO P 2100.1I, GSA Information Technology (IT) Security Policy , December 22, 2015. |
| ▪ GSA Order CIO P 2181.1, GSA HSPD-12 Personal Identity Verification and Credentialing, October 20, 2008. |
| ▪ GSA Order CIO 2104.1A, GSA IT General Rules of Behavior, June 5, 2012. |
| ▪ GSA Order CIO P 1878.1, GSA Privacy Act Program, September 2, 2014. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security 01-01, Revision 4, Identification and Authentication, May 30, 2015. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security 01-02, Revision 11, Incident Response, Incident Response, October 1, 2015. |
| ▪ GSA-IT Security Procedural Guide CIO-IT, Security 01-05, Revision 3, Configuration Management, July 14, 2015. |
| ▪ GSA-IT Security Procedural Guide CIO-IT Security 01-07, Revision 3, Access Control, April 1, 2015. |
| ▪ GSA-IT Security Procedural Guide CIO-IT Security 01-08, Revision 3, Audit and Accountability (AU) Guide, June 30, 2010. |
| ▪ GSA IT Security Procedural Guide CIO-IT November 3Security-05-29, Revision 4, IT Security Training and Awareness Program, November 3, 2015. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security-06-29, Revision 2, Contingency Planning, August 16, 2010. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security-06-30, Revision 7, Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA), May 31, 2011. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security 06-32, Revision 3, Media Protection Guide, April 15, 2012. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security 07-35, Revision 2, Web Application Security Guide, June 16, 2008. |
| ▪ GSA IT Security Procedural Guide 08-39, FY 2015 IT Security Program Management Implementation Plan, Revision 7, October 30, 2014. |

| Risk Management Framework Plan Applicable Documents |
|---|
| ▪ GSA IT Security Procedural Guide CIO-IT Security-09-44, Plan of Action and Milestones (POA&M) March 30, 2009. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security 10-50, Revision 2, Maintenance Guide, April 20, 2015. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security 11-51, Revision 2, Conducting Penetration Test Exercise Guide, December 11, 2014. |
| ▪ GSA IT Security Procedural Guide CIO –IT Security 12-63, GSA's System and Information Integrity, March 5, 2012. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security 12-64, Physical and Environmental Protection, March 30, 2012. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security-12-66, Information Security Continuous Monitoring Strategy, June 24, 2015. |
| ▪ GSA IT Security Procedural Guide CIO-IT Security-12-67, Securing Mobile Devices and Applications Guide, May 20, 2014. |
| ▪ GSA-IT Security Procedural Guide CIO-IT Security 14-69, SSL/TLS Implementation Guide, December 24, 2014. |
| ▪ Committee on National Security Systems Instruction No. 1253, Security Categorization and Control Selection for National Security Systems, March 12, 2014. |
| ▪ Committee on National Security Systems Instruction (CNSSI) No. 5000, Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony, April 2007. |
| ▪ Verizon, Corporate Policy Statement (CPS)-810, Information Security Policy. |
| ▪ Verizon, Corporate Policy Instruction (CPI)-810, Information Security Corporate Policy Verizon, Network Security Baseline (NSB) Standards and Practices. |
| ▪ Verizon Public Sector, Verizon Public Sector Information Security Program Plan. |

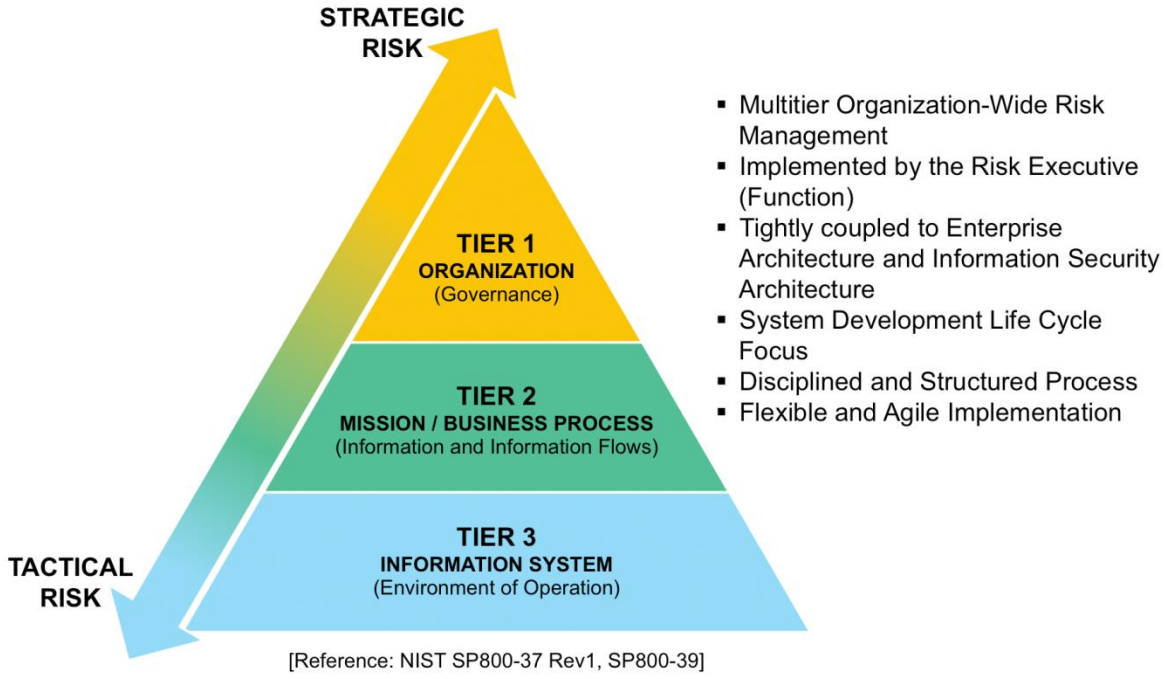
*Note: If the Verizon policies/procedures/standards are less stringent than the Federal policies/procedures/standards, Verizon will meet the Federal requirements.*

## 8.3 Organizational Risk Management Process Overview

### 8.3.1 Verizon Information Security Governance

Verizon addresses risk at various levels of the organization, with specific emphasis on the following three levels: Organization, Mission or Business, and Program or Information Systems. First, the Organization level, addresses security from a global Corporate Governance perspective; Second, the Mission or Business level is supported by the Verizon Public Sector team. The Verizon Public Sector team interfaces directly with the Government to address security issues and has optimized an organizational structure to support information risk management. Finally, the Program or Information System level implements Government requirements, and confirms program level information system risk management. A model of the Verizon Information Security Risk Management Governance is depicted in **Figure 8.3.1-1**.

**Figure 8.3.1-1. Verizon's Risk Management Process.**




Using this three-tiered approach, Verizon works to continuously improve Verizon's risk-related activities and effectively communicate within and between the three tiers to protect customer data. Verizon maintains a staff of experienced and credentialed professionals to ensure the ongoing support of Verizon's security posture as described in the following sections.

### 8.3.1.1 Verizon Organizational Wide Information Security.

[redacted]

[redacted]

[redacted]

[redacted]. The primary objectives of this Program include preventing, detecting, containing and remediating security breaches and the identification of the misuse of Verizon information resources. The Program also includes reporting, monitoring, and internal auditing to update Verizon senior management. The Information Security Program guides Verizon management of information security risks.

#### 8.3.1.2 Mission Level - Verizon Public Sector Information Security Support

Verizon Enterprise Solutions Public Sector (hereinafter referred to as "Verizon Public Sector") has established information security policies, procedures, and architectures to protect critical government systems and information resources. [redacted]

#### 8.3.1.3 Verizon Program Level Information Security Support

Verizon manages tactical risk at the information system level. [redacted]

### 8.3.2 Verizon Executive Information Security Leadership

#### 8.3.2.1 Chief Information [redacted]

[redacted]

#### 8.3.2.2 Chief Security Officer, [redacted]

[redacted]

#### 8.3.2.3 Chief Information Officer, [redacted]

[redacted]

[redacted]

### 8.3.2.4 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

## 8.3.3 Verizon Public Sector Support

Verizon Public Sector is dedicated to supporting the needs of its government customers and has created a security organization to align with those needs. This team augments Verizon security policies with government security requirements, including teams supporting policy, engineering, operations, IT and management created to support security and accountability to the Government. Verizon's corporate organizational structure depicted in **Figure 8.3.1.1-1** above, implements the NIST tiered risk management approach defined in NIST SP 800-37.

### 8.3.3.1 Senior Information Security Officer, [redacted]

[redacted]

### 8.3.3.2 Verizon Public Sector Chief Technology Officer, [redacted]

[redacted]

### 8.3.3.3 Verizon Public Sector Chief Program Officer, [redacted]

[redacted]

[redacted]

#### 8.3.3.4 Verizon Deputy Public Sector Chief Program Officer, [redacted]

[redacted]

#### 8.3.3.5 Information System Security Architect, [redacted]

[redacted]

#### 8.3.3.6 Information System Security Manager (ISSM), [redacted]

[redacted]

[redacted]

### 8.3.3.7 Common Control Provider

The Verizon Common Control function is provided [redacted]

[redacted]

### 8.3.3.8 Information System Owner, (Program-specific Assignment)

[redacted]

[redacted]

## 8.3.4 Program Level Support

At the program level Verizon supports the following organization functions.

### 8.3.4.1 Information System Security Engineer, [redacted]

[redacted]

[redacted] n **Table 8.3.4.1-1**.

**Table 8.3.4.1-1. Information Security Architect Responsibilities.**

[redacted]

[redacted]

vulnerabilities.

### 8.3.4.2 Information System Engineer, [redacted]

[redacted]

**Table 8.3.4.2-1. Information System Engineer Responsibilities.**

[redacted]

### 8.3.4.3 Information System Security Officer (ISSO)

The BSS ISSO plays a leading role in introducing appropriate, structured methodology to help identify, evaluate, and minimize risks to the BSS systems and mission. In concert with the ISSM, the ISSO acts as a major consultant in support of the BSS project management team to verify that this activity takes place on an ongoing basis. The BSS ISSO's duties are summarized in **Table 8.3.4.3-1**.

[redacted]

## 8.4 Information System Overview

Verizon will provide and maintain BSS to meet the requirements of the EIS contract as identified in RFP Section G.6.5.4. Key components are included in **Table 8.4-1**.

**Table 8.4-1. BSS Component Service Requirements.**

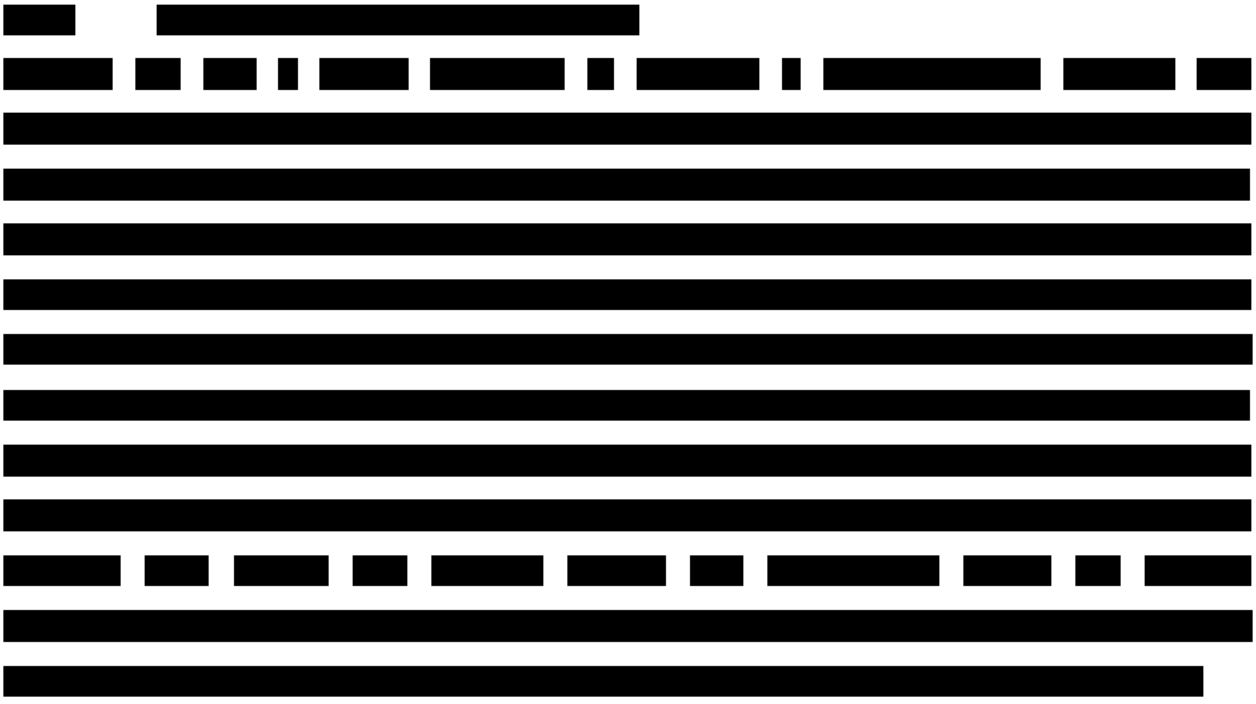
| Service | Minimum Functionality |
|---|---|
| **Customer Management** | ▪ User Training ▪ Trouble Management |

| Service | Minimum Functionality | |
|---|---|---|
| **Financial Management** | ▪ Billing Management<br>▪ Disputes | ▪ SLA Credit Management<br>▪ Payment Tracking |
| **Order Management** | ▪ Order Submission | ▪ Order Tracking |
| **Inventory Management** | ▪ Inventory Management | |
| **Service Management** | ▪ Service Assurance | ▪ SLA Management |
| **Program Management** | ▪ Administration<br>▪ Project Management | ▪ Reporting<br>▪ Service Catalog |

The EIS RFP encourages the use of commercial systems to meet the BSS requirements and indicates the BSS can be architected with a single BSS, an integrated BSS, or a combination of BSS's.

### 8.4.1 Verizon Commercial BSS

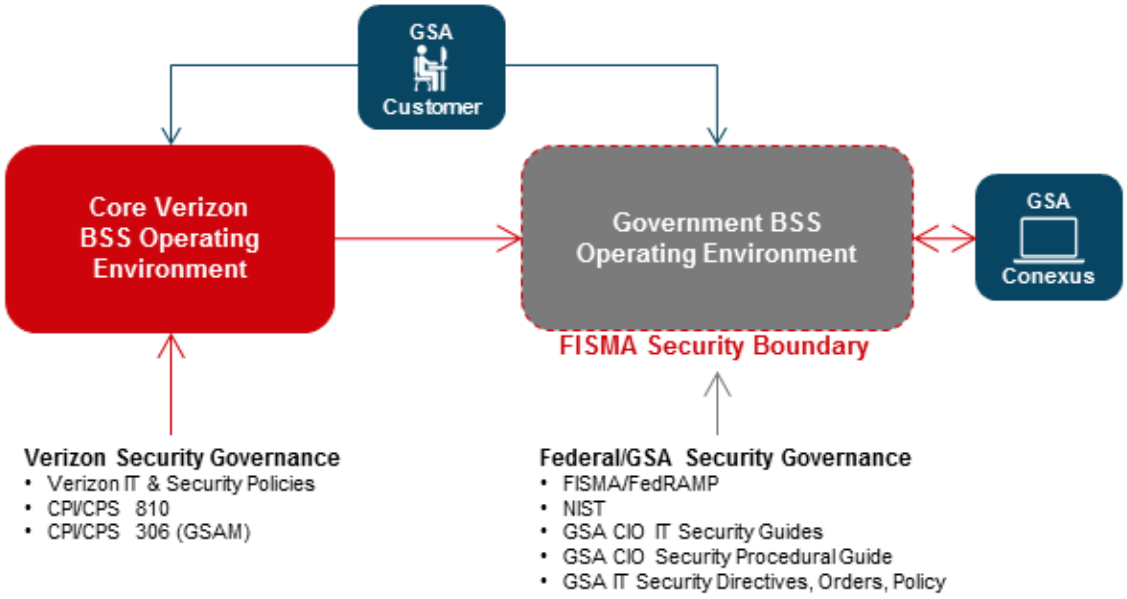
As one of the largest commercial telecommunications providers in the world, Verizon has internal back-end support systems in place to provide service requirements for countless customers, including the Federal government. In fact, Verizon's commercial BSS incorporates industry leading and proven IT platforms capable of processing, managing, deploying and supporting large scale service orders of many types of services for countless customers simultaneously across a large number of contracts.



## 8.4.3 [redacted]

[redacted]

**Figure 8.4.3-1. BSS Operating Environments.**

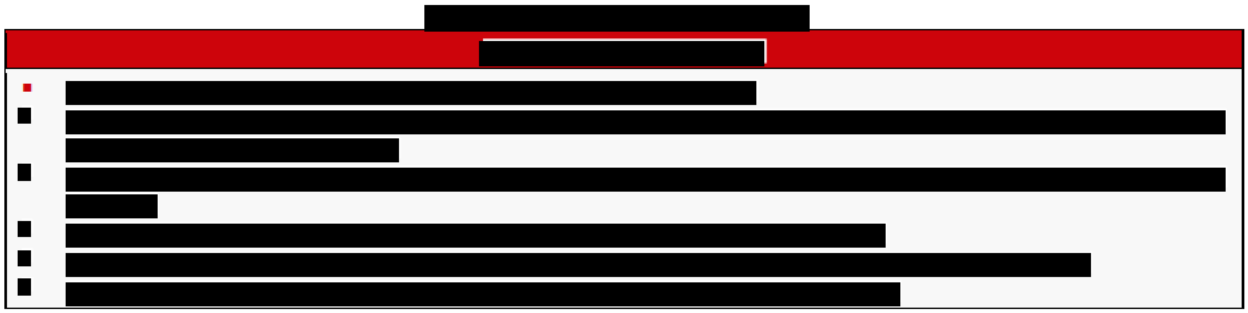



## 8.4.4 [redacted]

[redacted]

[redacted]. Verizon was the first Service Provider in the U.S. to achieve an ISO/IEC 20000-1 Information Technology Service Management System Registration.

[redacted]



[redacted]

#### 8.4.1.1 FISMA-Compliant Government BSS

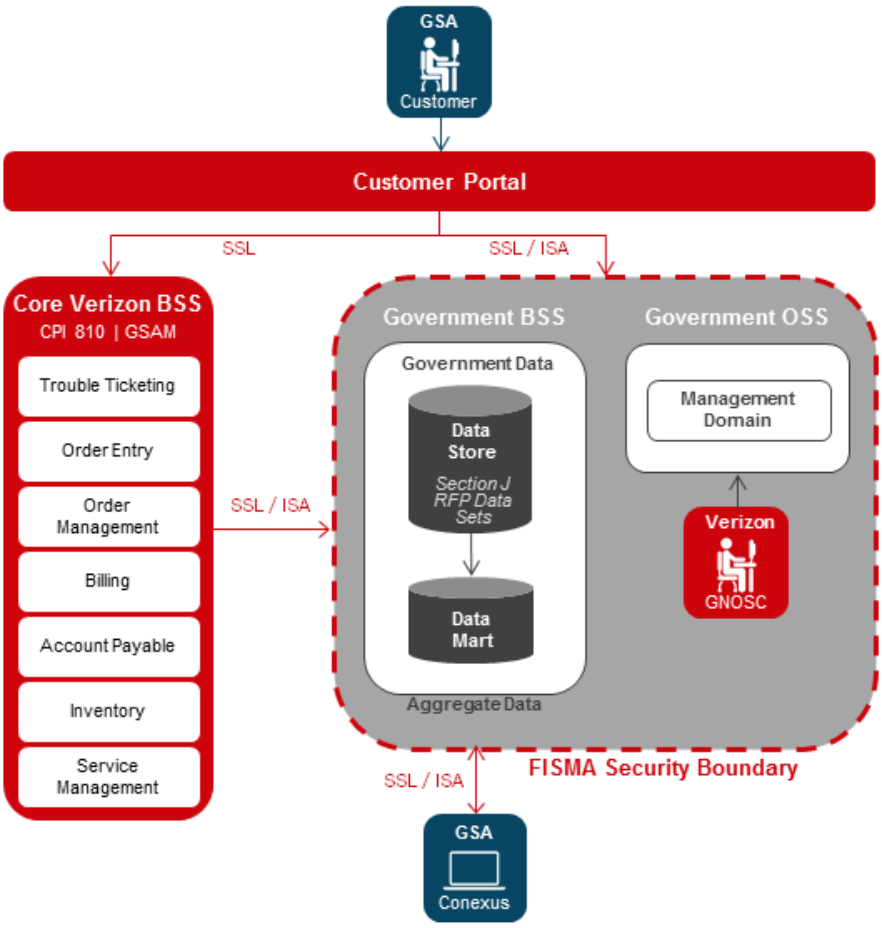
The Government BSS will be a secured operating environment bridging BSS component services between the Verizon and GSA BSS platforms. The Government BSS will incorporate Government data and access to the data. The Government BSS will be a fully dedicated operating environment custom developed for the EIS contract, with the objective to meet Federal and GSA security and operation requirements and guidelines. This Government BSS operating environment will be built in compliance with FISMA Moderate impact level, and in support of the NIST Risk Management Framework processes. This dedicated environment will be used to validate and support applicable federal and agency-specific IT security directives, standards, policies, and reporting

requirements, as well as A&A activities for the ATO effort. The Government BSS will be governed by FISMA associated guidance and directives such as Federal Information Processing Standards (FIPS) and NIST Special Publication (SP) 800 series guidelines, GSA IT security directives, policies and guidelines, as well as other appropriate Government-wide laws and regulations for protection and security of Government IT as outlined in the Applicable Standards and Guideline section (**Section 8.2, Table 8.2-1**).

## 8.5 BSS Architectural Description

### 8.5.1 Government BSS Architecture and Service Description

[redacted]



#### 8.5.1.1 Customer Delivery Channels Tier

The Customer Delivery Channel tier consists of the delivery and data exchange methods and controls required to send or exchange data and deliverables between Verizon Government BSS and GSA Conexus. [redacted]

#### 8.5.1.2 Government Data Tier

The purpose of the Government Data Tier is to provide a repository to protect and manage Government-specific sensitive data and deliverables, as specified in RFP Section J. [redacted]

#### 8.5.1.3 Verizon BSS Tier

The Verizon BSS is comprised of many collective sets of technology, tools, processes, and resources that perform order processing, provisioning, service management, notification, billing, and payment processing. Verizon has invested heavily in the development of the BSS initiative to simplify and accelerate the service ordering and enablement processes. The Verizon BSS program has successfully developed and deployed an innovative next-generation BSS for its customers. The Verizon BSS improves quoting, ordering, provisioning, and simplifies billing, which will reduce the overall time from quote to implementation. The system is designed to provide flow-through automation and data validation to reduce defects and billing errors. The BSS platform has been honored by the TM Forum for contributing to enterprise business

transformation. Third-party TM Forum testing has concluded that Verizon's BSS closely conformed to Business Process Framework V.13.5. [redacted]

#### 8.5.1.4 Verizon Government BSS A&A Boundary

[redacted]

#### 8.5.1.5 Verizon Government BSS A&A Process

Verizon follows the security requirements as mandated in FIPS 200 and applies security controls in accordance with NIST Special Publication 800-53. For formal Authorization to Operate (ATO) approval, Verizon will use NIST SP 800-37 as guidance for performing the security A&A process. The level of effort for the security assessment and authorization is based on the system's categorization per NIST Federal Information Processing System (FIPS) Publication 199. Verizon will complete the Government BSS SSP in accordance with NIST Special Publication 800-18, Rev. 1 (hereinafter listed as NIST SP 800-18) and other relevant guidelines. [redacted]

[redacted]

This Government BSS operating environment will be built in compliance with FISMA Moderate impact level, and in support of the NIST Risk Management Framework processes. This dedicated environment will be used to validate and support the applicable Federal and Agency-specific IT security directives, standards, policies, and reporting requirements, as well as A&A activities for the ATO effort. The Government BSS will be governed by FISMA associated guidance and directives such as Federal Information Processing Standards (FIPS) and NIST Special Publication (SP) 800 series guidelines, GSA IT security directives, policies and guidelines, as well as other appropriate Government-wide laws and regulations for protection and security of Government IT as outlined in Section 8.4 BSS Information System Overview.

## 8.6 The Verizon BSS RMF Process

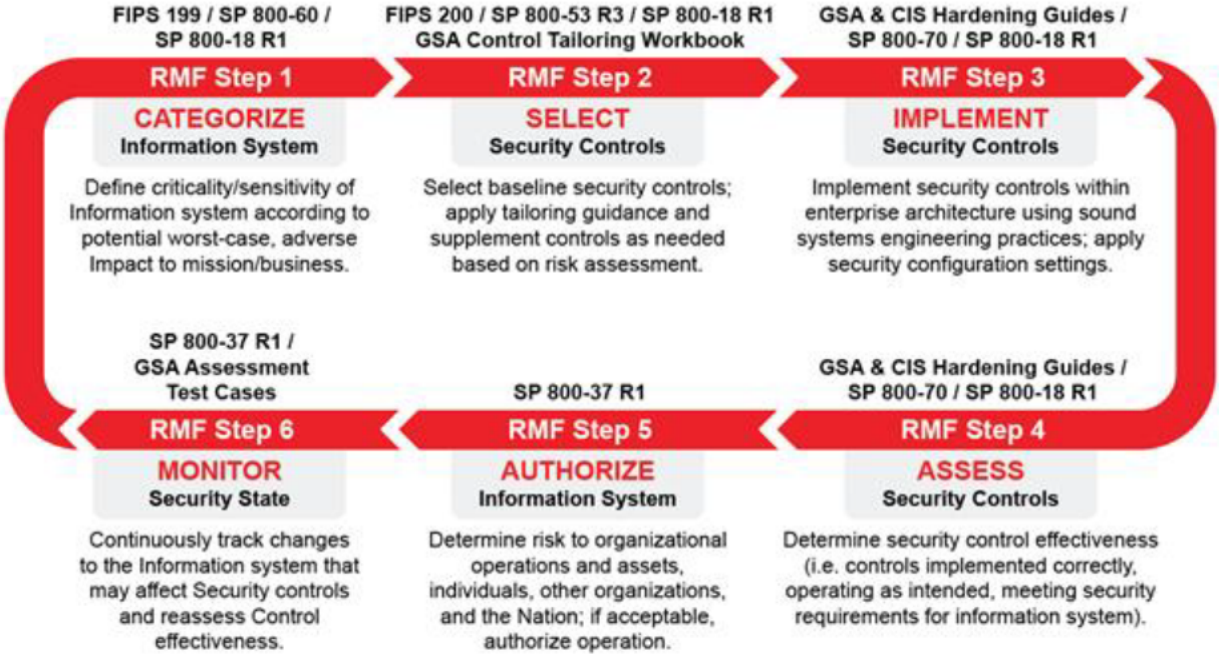
For more than 10 years Verizon has followed the Security Authorization Process (formerly Certification and Accreditation (C&A)) process defined in GSA CIO-IT Security-06-30 Managing Enterprise Risk - Security Assessment and Authorization, Planning, and Risk Assessment. As specified in Rev. 7 of GSA CIO-IT Security-06-30, the Verizon BSS RMF process is based on the NIST Risk Management. The process is a documented, repeatable framework that is central to the System Development Life Cycle (SDLC) that will be used for BSS. As defined in NIST SP 800-37 and GSA CIO-IT Security-06-30 (as illustrated in **Figure 8.6-1)**, the RMF steps that Verizon will follow for BSS are outlined in **Table 8.6-1** at a minimum.

**Table 8.6-1. Verizon RMF Steps.**

| RMF Step | Step Description |
|---|---|
| **RMF Step One** | Categorize Information System in accordance with FIPS 199, NIST SP 800-60, and NIST SP 800-18 R1 when applicable. |
| **RMF Step Two.** | Select Security Controls in accordance with FIPS 200, NIST SP 800-53 R4, NIST SP 800-18 R1, and the GSA and Verizon Control Tailoring Workbook (or comparable customer Agency document). |
| **RMF Step Three** | Implement Security Controls in accordance with customer Agency & Center for Internet Security (CIS) Hardening Guides, NIST SP 800-70, and NIST SP 800-18 R1. |
| **RMF Step Four** | Assess Security Controls in accordance with NIST SP 800-53A R4 and Verizon policy, GSA Assessment Test Cases and NIST SP 800-18 R1. |
| **RMF Step Five** | Authorize Information System in accordance with NIST SP 800-37 R1. |
| **RMF Step Six** | Monitor Security Controls in accordance with NIST SP 800-37 R1, NIST SP 800-137, and GSA Assessment Test Cases. |

The output of the Verizon BSS RMF process includes an understanding of the risk associated with the system and the security authorization artifacts, also known as the Body of Evidence (BoE). To complete the authorization process, the BoE is submitted as part of the Security Authorization Package. The GSA AO will use the Security Authorization Package to evaluate whether deployment of the IS presents, or maintains an acceptable level of risk to organizational operations, assets, individuals, other organizations, and the Nation.

**Figure 8.6-1. Verizon BSS Risk Management Framework Process.**




[Reference: NIST SP 800-37 Rev 1, SP800-39]

The remainder of this section will detail how Verizon will accomplish each of the six RMF steps during the BSS security life cycle.

### 8.6.2 RMF Step One – Categorize Information System

The first step of the Verizon BSS RMF is the categorization of the Information System. Verizon utilizes the FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems to accurately categorize each Verizon system that processes Government information. The final impact level (Low, Moderate, or High) will affect the remaining steps in the process. The initial system categorization effort involves system stakeholders, which includes Verizon and Government personnel. Considerations include applicable legislation, policies, directives, regulations, and mission needs that must be accounted for and documented prior to mapping these requirements to the security categories outlined in the FIPS 199.

**Table 8.6.2-1** below lists the supporting tasks associated with RMF Step One, the primary roles associated with each task, and the task deliverables. As defined in NIST SP 800-53, the Information System Owner is the official responsible for the overall procurement, development, integration, modification, operation and maintenance of an information system.

**Table 8.6.2-1. RMF Step One Supporting Tasks.**

| Supporting Tasks | Primary Responsibility | Deliverables |
|---|---|---|
| **Task 1-1**—Categorize the Information System and document the results in the SSP. | Information System Owner (ISO) - Verizon | Draft SSP with System Categorization |
| **Task 1-2**—Describe the information system (including system boundary) and document the description in the SSP. | Information System Owner (ISO) - Verizon | Updated SSP to include a description of the IS |
| **Task 1-3**—Register the IS with the appropriate organizational program management offices. | Information System Owner (ISO) - Verizon | Document or entry in the IT registry with the official system name, system owner, and categorization |

**TASK 1-1: Security Categorization.** Information and Information Systems are categorized according to the potential impact to Verizon and the Government of a loss of a system's Confidentiality, Integrity, and/or Availability. **Figure 8.6.2-1** below defines the three security objectives for information and information systems, and also identifies what would constitute a loss for each objective.

**Figure 8.6.2-1. C-I-A Security Objectives (44 U.S.C., Section 3542).**

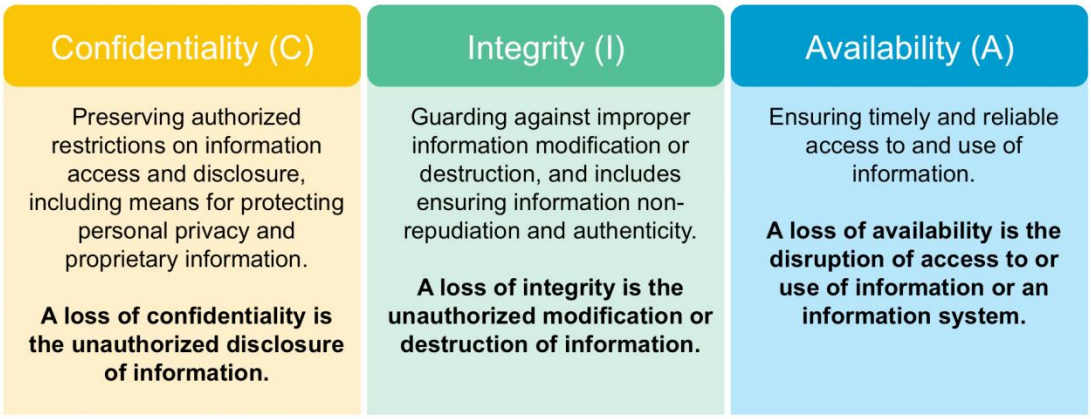
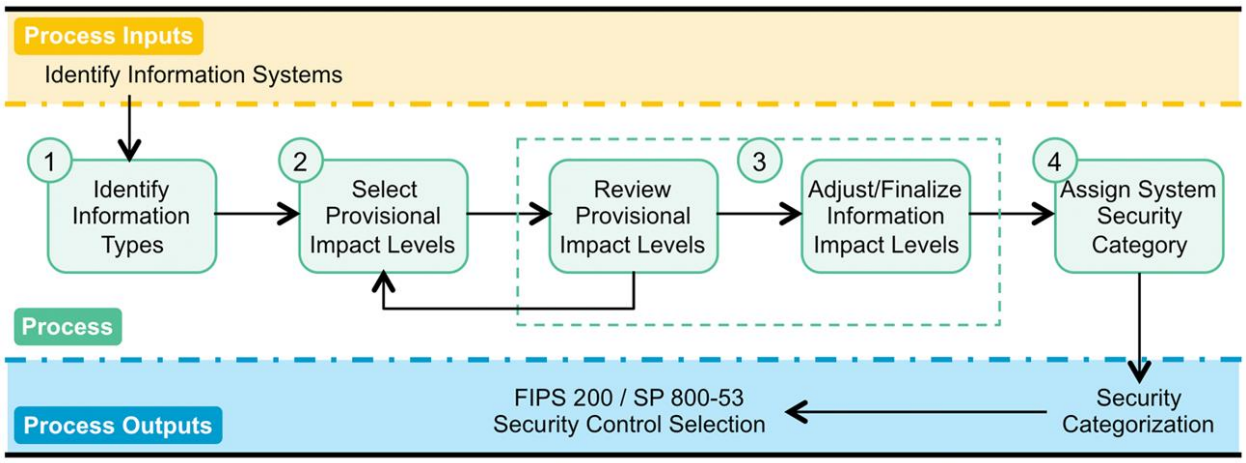



**Figure 8.6.2-2** shows the security categorization process defined in NIST SP 800-60 that Verizon follows. This four-step security categorization process drives the selection of baseline security controls and helps determine the information system's CIA security objectives.

**Figure 8.6.2-2. Security Categorization Process.**




[Reference: NIST SP800-60 Rev1]

**Figure 8.6.2-3** shows the three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability.

**Figure 8.6.2-3. FIPS 199 Categorization Definitions: Potential Impact Levels.**

| Low | Moderate | High |
|---|---|---|
| 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, individuals, other organizations, or the national security of the United States. | 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, individuals, other organizations, or the national security of the United States. | 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, individuals, other organizations, or the national security of the United States. |

**TASK 1-2: Information System Description.** Once the FIPS 199 system categorization is completed per Task 1-1, Verizon prepares a description of the information system (including system security boundary) and documents the description in a System Security Plan (SSP), based on NIST SP 800-18 R1. The SSP provides an overview of the security requirements for the information system and describes the security controls put in place or planned for meeting the system's defined security requirements. During this phase of the Verizon BSS RMF, the following SSP sections will be completed in detail, and provided to the BSS AO to support an authorization decision:

indicates if there is an Interconnection Security Agreement (ISA) and/or Memorandum of Understanding/Agreement (MOU/MOA) on file; date of agreement to interconnect; FIPS 199 category; authorization to operate status; and the name of the authorizing official. Interconnections will be documented in accordance with GSA IT Security Policy 2100.1 or comparable customer agency document and NIST SP 800-47.

**TASK 1-3: Information System Registration.** Once the SSP and supporting documentation (e.g., the Security Assessment Boundary and Scope Document) is completed, Verizon will register the information system with the appropriate GSA organizational program/management offices and security personnel. This system registration will complete the activities required to categorize the information system under Step1 of the RMF. The output of the security categorization activities conducted during RMF Step One will be used as the input to RMF Step Two, in which Verizon determines the selection of the appropriate NIST 800-53 R4 security control baseline (Low-, Moderate-, or High-impact) for the BSS information system.

### 8.6.3 RMF Step Two – Select Security Controls

As previously discussed, based on the FIPS 199 impact level (Low -, Moderate-, or High-impact as determined in RMF Step One), Verizon will select the appropriate security controls for the information system as defined in FIPS 200 and the companion guide NIST 800-53 R4 Minimum Security Controls for Federal Information Systems. In RMF Step Two, Verizon determines common controls, and identifies these security controls as system-specific, hybrid, or inherited. Security controls are tailored and supplemented as necessary with additional controls and/or control enhancements to address unique organizational or system-specific risks. Based on the security control selection, Verizon will update its current continuous monitoring strategy, and gain GSA Authorizing Official approval of the SSP.

**Table 8.6.3-1** below describes the supporting tasks, roles associated with each task, and the task deliverables for RMF Step Two — Select Security Controls.

**Table 8.6.3-1. RMF Step Two – Select Security Controls.**

| Supporting Tasks | Primary Responsibility | Deliverables |
|---|---|---|
| **Task 2-1**—Identify the security controls that are provided by the organization as common controls for organizational IS and document the controls in the SSP. | Common Control Provider (CCP); ISO,ISSM/ISSO, ISSA, - Verizon Security Control Assessor (SCA) –ordering agency or Independent Contractor | Document the common controls in the SSP |
| **Task 2-2**—Select the security controls for the IS (i.e. baseline, overlays, tailored) and document the controls in the SSP. | ISO; ISSA - Verizon | Document the selected security controls in the Draft SSP, Control Summary Table, and/or Control Tailoring Workbook |
| **Task 2-3**—Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the IS and its environment of operation. | ISO or CCP - Verizon | Documented and approved Continuous Monitoring Plan/Strategy including frequency of monitoring for each control |
| **Task 2-4**—Review and approve the draft SSP by the AO or DAO. | AO or DAO –ordering agency ISSM/ISSO - Verizon | Documented and approved Draft SSP, Control Summary Table, and/or Control Tailoring |

**TASK 2-1: Common Control Identification.** The first task in the Verizon BSS RMF Step Two is to identify the security controls that are provided by Verizon as common controls and document these controls in the SSP prepared in RMF Step One. Verizon documents the implementation of the controls in the BSS SSP and, as appropriate, references the controls contained in the security plans of the common control providers. In selecting common controls, the Verizon System Owner (whose systems are inheriting the controls) will review the SSP, Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), or other security-relevant information for common controls (or a summary of such information).

Once the common controls are identified, Verizon begins completing the GSA NIST SP 800-53 R4 Control Summary Table for a Moderate Impact Baseline for the BSS system. This table identifies controls types (common vs. hybrid controls vs. app specific controls) with implementation status (fully implemented, partially implemented, planned, etc.). Throughout the remainder of the BSS life cycle, Verizon will maintain and update the Control Summary Table to accurately reflect the implementation status of each NIST SP 800-53 security control and enhancement.

**TASK 2-2: Security Control Selection**. Selecting the initial control set, or baseline, is the process of grouping the appropriate column of controls that correspond to the security categorization of the system as identified in RMF Step One.

Once the security categorization has been determined, the initial set of security controls may then be selected from the appropriate authoritative catalog of security controls

(e.g., NIST SP 800-53 as outlined in **Table 8.2-1**) based on the corresponding security categorization of Low, Moderate, or High.

While the selected security controls normally apply, in many cases, some of the controls may be considered to be “inherited” from hosting organizations or elements within the organization. An example of this is physical security controls such as perimeter fences, security guards, camera monitoring systems and security badge systems, as well as environmental controls. Environmental controls may include humidity controls and fire prevention and suppression systems that may already be established and provided as an organizational service for multiple systems. These “inherited” controls are included in the overall selection. However, as discussed in subsequent sections, this provision greatly simplifies some aspects of the documentation and security control implementation process. The BSS system has been categorized as a FISMA Moderate impact system. As a result of this categorization, and as previously described, the security control baseline originates with control guidance as specified in NIST SP 800-53. The controls identified in the security control baseline can subsequently be tailored according to supplemental guidance provided by both Verizon and ordering agency’s assessment of risk as well as the local conditions within Verizon’s geographically diverse locations. Verizon and GSA will utilize the GSA Control Tailoring Workbook as a tool to confirm that BSS security controls and enhancements are correctly selected.

Although it is not anticipated for the BSS, Verizon will also include any applicable security control overlays to complement security control baselines and parameter values in NIST SP 800-53 (refer to **Table 8.2-1**). After selecting the initial set of baseline security controls, Verizon will work with GSA to determine if the security control baselines selected require tailoring to modify and align the controls more closely with the specific conditions within the BSS operational environment. Verizon will explicitly document in SSP control tailoring decisions, including the specific rationale (mapping to risk tolerance) for those decisions. Selected controls will be accounted for in the SSP. If a selected control is not implemented or is not applicable, then the rationale for not implementing the control will be fully documented.

In some cases, additional security controls or control enhancements may be needed to address specific threats to, or vulnerabilities within a system or to satisfy the requirements of public laws, Executive Orders, directives, policies, standards, or regulations. Risk assessment at this stage in the security control selection process provides important inputs for determining the sufficiency of the tailored set of security controls. The inclusion of each control is based on the need to reduce risk to an established tolerance level. Once the security control set is selected, Verizon will complete the initial version of the GSA NIST SP 800-53 R4 Control Tailoring Workbook, which identifies the ordering agency's organizational defined settings for each security control and enhancement. Verizon will note in column E of the workbook where the settings implemented for the BSS are different from the GSA Defined Setting (in column D). Any deviations from the GSA Defined Settings will be submitted with the System Security Plan in Task 2-4 (see below) for approval and acceptance by the GSA AO.

**TASK 2-3: Monitoring Strategy.** As part of the RMF process, Verizon documents the strategy for the continuous monitoring of the BSS security control effectiveness and any proposed or actual changes to the information system and its environment of operation. This strategy is based on the continuous monitoring capability that Verizon has been implementing for Government systems for over ten years.

As an output of this task, Verizon will prepare and deliver to GSA the BSS Continuous Monitoring Plan that documents how continuous monitoring of BSS will be accomplished in accordance with GSA IT Security Procedural Guide CIO-IT Security-12-66, Information Security Continuous Monitoring Strategy. The BSS Continuous Monitoring Plan will form the basis of the activities that Verizon will conduct during RMF Step Six (Monitor Security Controls). The Verizon continuous monitoring program will provide the GSA AO with a current understanding of the security state and risk posture of the BSS system. This understanding will enable the AOs to make credible risk-based decisions regarding the continued BSS operations and to initiate appropriate responses as needed when changes occur.

**TASK 2-4: Security Plan Approval.** Verizon's submission of the SSP will be the culmination of RMF Step Two, along with the completed Control Summary Table and

the Control Tailoring Workbook to the GSA. This will enable the ordering agency's ISSM/ISSO and the AO, with support from the Office of the Senior Agency Information Security Officer (OSAISO), to determine if the plan is complete, consistent, and meets the security requirements for the information system. Based on the results of the ordering agency's review, the SSP may require further updates prior to GSA final approval. The AO or designated representative, by approving the security plan, agrees to the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system; allowing Step Three of the RMF to begin.

The AO, or designated representative, must accept the SSP before security controls can be implemented and/or assessment activities can begin. By approving the security plan, the AO (or designated representative) agrees to the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system; allowing Step Three of the RMF to be completed.

### 8.6.4 RMF Step Three – Implement Security Controls

During RMF Step Three, Verizon implements the security controls selected in RMF Step Two consistent with NIST SP 800-53 and the approved System Security Plan. **Table 8.6.4-1** lists supporting tasks, the roles with primary responsibility for each task, and the task deliverables for Step Three—Implementing Security Controls.

**Table 8.6.4-1: RMF Step Three – Implement Security Controls.**

| Supporting Tasks | Primary Responsibility | Deliverables |
|---|---|---|
| **Task 3-1**—Implement the security controls specified in the SSP. | ISO or CCP – Verizon | N/A |
| **Task 3-2**—Document the security control implementation, as appropriate in the SSP, providing a functional description of the control implementation. | ISO or CCP;<br>ISSM/ISSO;<br>ISSE – Verizon | Updated SSP with information describing how security controls are implemented. |

**TASK 3-1: Security Control Implementation.** Security control implementation will be consistent with the ordering agency's enterprise architecture and information security architecture. Verizon configures and hardens the IT system using GSA IT security hardening guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as deemed appropriate by the Authorizing Official.

Implemented checklists are integrated with Security Content Automation Protocol (SCAP) content. Verizon conducts initial security control assessments (also referred to as developmental testing and evaluation) during information system development and implementation. This testing is conducted in parallel with the development and implementation of the system, thereby facilitating the early identification of weaknesses and deficiencies and providing the most cost-effective method for initiating corrective actions.

**TASK 3-2: Security Control Documentation.** During system implementation, Verizon documents the security control implementation in the SSP, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs). Security controls are documented in Section 13 of the SSP and are presented per the requirements in NIST 800-18. The following describes how the BSS NIST 800-53 R4 Moderate Impact Baseline security controls, security control enhancement, and supplemental controls will be implemented, including:

- The security control title;
- How the security control is being implemented or planned to be implemented;
- Any scoping guidance that has been applied and what type of consideration;
- The control type (Common, Hybrid, App Specific);
- Implementation status (e.g., implemented, partially implemented, planned, N/A);
- Definition of who is responsible for the security implementation.

The updated SSP formalizes plans and expectations regarding the overall functionality of the information system. Security control implementation descriptions include planned inputs, expected behavior, and expected outputs where appropriate, especially for technical controls. The SSP also addresses platform dependencies and includes additional information needed to describe how the security control can be achieved at the level of detail sufficient to support control assessment in RMF Step Four.

### 8.6.5 RMF Step Four – Assess Security Controls

After security controls are implemented, they must be evaluated. Upon implementation of security controls in RMF Step Three, a security control assessment is performed to determine the extent to which security controls are implemented correctly, operating as

intended, and producing the desired outcome with respect to meeting security requirements. The BSS Security Control Assessment (SCA) will be performed in accordance with NIST SP 800-53A, using the GSA NIST SP 800-53 R4 Security Assessment Test Cases. **Table 8.6.5-1** lists the tasks required to determine in place security controls, prepare the Security/Risk Assessment Report (SAR), and initiate corrective actions based on the findings and recommendations in the SAR.

**Table 8.6.5-1: RMF Step Four – Tasks, Responsibilities, and Deliverables.**

| Supporting Tasks | Primary Responsibility | Deliverables |
|---|---|---|
| **Task 4-1**—Develop, review, and approve a plan to assess the security controls. | ISSM/ISSO; ISSE - Verizon<br>SCA – GSA or Independent Contractor | Security Assessment Plan |
| **Task 4-2**—Assess the security controls in accordance with the assessment procedures defined in the Security Assessment Plan. | SCA – GSA or Independent Contractor | Individual test results for each test or matrix for tests |
| **Task 4-3**—Prepare the SAR documenting the issues, findings, and recommendations from the security control assessment. | SCA – GSA or Independent Contractor | SAR |
| **Task 4-4**—Conduct initial remedial actions on security controls based on the findings and recommendations of the SAR and reassess remediated control(s), as appropriate. | ISO or CCP;<br>ISSM/ISSO – Verizon<br>SCA – GSA or Independent Contractor | SAR |

In accordance with Section C.2.8.4.5.4 of the EIS RFP, the Government is responsible for conducting the Security/Risk Assessment and Penetration Tests. In accordance with Penetration Test Rules of Engagement, [redacted] Review activities will include operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Government information. The following paragraphs detail each task that will be performed during RMF Step Four.

**TASK 4-1: Assessment Preparation.** Verizon will assist in the assessment preparation by providing the Government's Security Control Assessor with the information required to develop and receive authorization approval from the GSA AO for the Security Assessment Plan (SAP) for assessing the BSS security. The purpose of the Security Assessment Plan approval is two-fold: (i) to establish the appropriate expectations for the security control assessment; and (ii) to bound the level of effort for the security control assessment. The Security Assessment Plan provides system background

information, the objectives for the security control assessment, the assessment approach, and the assessment test cases to be used in Task 4-2. The BSS security control assessment will be based on the GSA 800-53 R4 Assessment Test Cases. Additional assessment test cases (from the GSA Assessment Test Cases) may be added for any supplemented controls and/or control enhancements added during Task 2-2 to address unique organizational and/or system specific needs. As specified in GSA IT Security Procedural Guide 06-30, the security assessment requirements listed in **Table 8.6.5-2** will be defined in the Security Assessment Plan and implemented for information systems per its FIPS 199 impact level. As a Moderate impact information system:

The Security Assessment Plan will be reviewed by the Verizon System Owner, ISSO, and ISSM and approved by the GSA AO to verify that the plan includes the above requirements, is consistent with system/organizational security objectives, employs required assessment tools and techniques, assessment test cases, and automation to support the concept of continuous monitoring and near real-time risk management.

**Security Control Assessment.** During this RMF task, the Government independent third-party assessment organization will assess the BSS security controls following the Security Assessment Plan and using the GSA Assessment Test Cases updated in Task 4-1 to determine if the controls implemented in RMF Step Three are operating as

intended and producing the desired outcome with respect to meeting the security requirements for the information system. The IT Security Assessment is typically conducted using a three-phased approach as outlined in **Figure 8.6.5-1**.

**Figure 8.6.5-1. Typical IT Security Assessment Methodology.**


As illustrated above, a typical security control assessment is conducted in three phases, the Pre-assessment, On-site Security Assessment and the Analysis & Reporting as described in **Table 8.6.5-3**:

**Table 8.6.5-3. Security Control Assessment Phases.**

| Security Control Assessment Phases |
|---|
| **Phase 1 Pre-Assessment Phase.** During the Pre-Assessment phase, the Information System Security Manager and the Security Assessment Team plan necessary details of the IT security assessment. This activity confirms that the scope of the assessment is mutually agreed upon, the assessment schedule and on-site plan are defined, information is shared with key stakeholders, and logistical issues are addressed. This phase verifies that the assessment will be carried out in an efficient manner and the goals and objectives of the assessment will be satisfied. Generally, the Pre-Assessment activities begin approximately four weeks in advance of the On-site Security Assessment Phase. |
| **Phase 2 On-Site Security Assessment Phase.** The on-site phase of the assessment typically takes a week to complete. During the on-site assessment, the Security Assessment Team reviews key documentation provided by the staff, interviews key personnel, and performs network vulnerability scanning and technical security configuration reviews based on the scope defined during the Pre-Assessment Phase. Scans will be performed as an authenticated user with elevated privileges. The Security Assessment Team also evaluates current practices based on the recommended IT security safeguards descr bed within the NIST and GSA Information Security Framework. The Security Assessment Team also evaluates the management, operational, and technical safeguards currently in place in order to determine where risk is present, ad meets with stakeholders to discuss any preliminary observations made during the assessment, to answer any questions they may have, and to identify the next steps within the security assessment process. |
| **Phase 3 Analysis and Reporting.** Following the conclusion of the on-site assessment activities, the Security Assessment Team performs detailed analysis of the information collected and observations made to develop detailed, actionable risk mitigation recommendations. Observations and recommendations are presented in a prioritized order based on the estimated risk. For each of these vulnerabilities, the report provides recommendations to either eliminate or reduce the risk presented by the vulnerability. Once the on-site assessment has been completed, a draft will be provided to GSA in approximately three to four weeks. GSA will then have the opportunity to review and comment on the draft. Delivery of the final report should take place approximately two weeks after the comment period is closed. |

**TASK 4-3: Security Assessment Report.** At the completion of the assessment, the Independent Security Control Assessor prepares the SAR that documents the issues, findings, and recommendations from the security control assessment. The SAR includes assessment findings with recommendation(s) and risk determinations from the NIST 800-30 risk assessment, and identifies and discusses Critical, High and Moderate

operating system, web application, and database scan/configuration vulnerabilities. Low risk findings do not have to be individually identified; however a reference is provided as to where they can be found in the appendix of the Security Assessment Report. Risk is determined for both individual findings and the overall system or application. The risk determination will be included as part of the authorization package. The contents of the SAR risk assessment is detailed in **Table 8.6.5-4**.

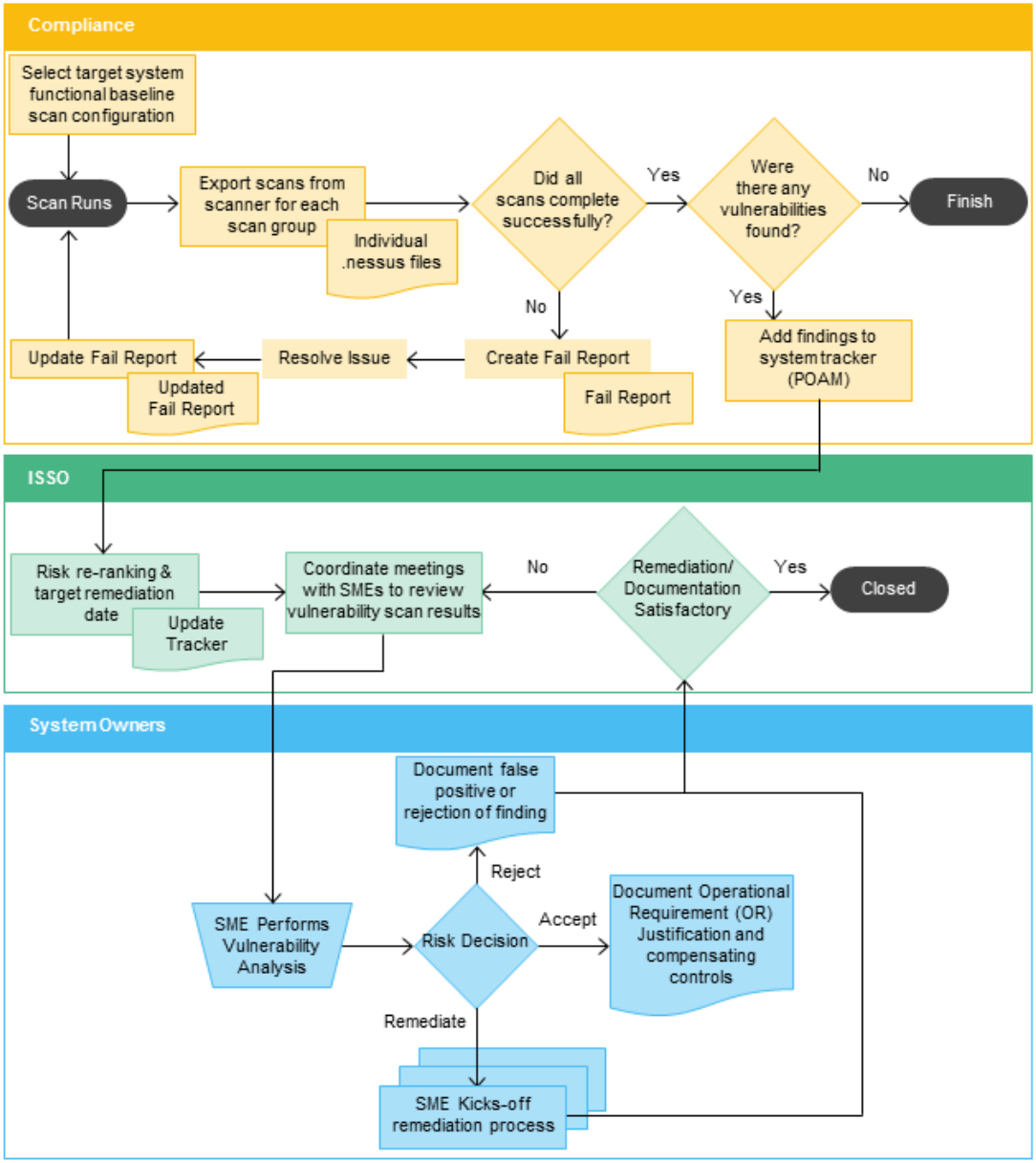
**Table 8.6.5-4. Security Assessment Report Risk Assessment Contents.**

| SAR Risk Assessment |
|---|
| ▪ Developing the list of threats to the system. The list should include hackers, malicious insiders, attacks against the system facility, and natural disasters.<br>▪ Developing Vulnerability/Threat Pairings.<br>▪ Assessing each system instance of absent controls and/or vulnerabilities identified during the Security Assessment.<br>▪ Evaluating the likelihood that one of the identified threats will exploit an identified vulnerability.<br>▪ Assessing the poss ble impact to the system and the agency if the vulnerability was exploited.<br>▪ Making a determination of risk based on the likelihood that the threat will exploit the vulnerability, and the impact that would result.<br>▪ Evaluating the risks of identified vulnerabilities to determine an overall level of risk for the system or application. |

The SAR also documents findings from the security assessment and its likelihood, impact, and risk discussion/rating, and recommended control for correcting deficiencies in security controls.

**TASK 4-4: Remedial Action.** Following the conclusion of reporting activities, Verizon immediately begins security control remediation efforts based on the findings and recommendations of the SAR and reassess remediated control(s), as appropriate. The ISSO will manage the remediation efforts by leveraging the ordering agencies' and Verizon's Plan of Action and Milestone (POA&M) process. If a critical/high vulnerability is discovered, it is remediated, or has the severity level reduced to "medium" or "low" within 30 days. Moderate vulnerabilities must be remediated or have the severity level reduced to "low" within 90 days. **Figure 8.6.5-2** illustrates the process that Verizon uses to analyze and remediate security vulnerabilities.

**Figure 8.6.5-2. Vulnerability Analysis and Remediation Process.**




With the help of the Security Assessor, the SAR will be updated as findings are remediated. The Security Assessment determines the risk to Agency operations, Agency assets and individuals and, if deemed acceptable by the GSA AO (or designated representative), the Security Authorization in RMF Step Five will formalize the SCA's assessment with the GSA AO's (or designated representative) acceptance to authorize operation of the Information System.

### 8.6.6 RMF Step Five – Authorize Information System

The Verizon BSS RMF Step Five identifies weaknesses or deficiencies to be corrected and any residual vulnerabilities and submission of the security authorization package to the GSA AO (via the SCA) for adjudication. The Security Authorization will formalize the AO's acceptance (or not) to authorize operation of the Information System. **Table 8.6.6-1** lists supporting tasks, the roles associated with each task, and the task deliverables for Step 5 of the RMF.

**Table 8.6.6-1. RMF Step Five – Authorize Information System.**

| Supporting Tasks | Primary Responsibility | Deliverables |
|---|---|---|
| **Task 5-1**—Prepare the POA&M based on the findings and recommendations of the SAR, excluding any remediation actions taken. | SCA (document initial findings) -– Independent Contractor ISO (completes POA&M; adds additional items; includes CCP, if finding is against a common control) - Verizon | POA&M |
| **Task 5-2**—Assemble the Security Authorization Package to include Artifacts and submit the package to the AO for adjudication. | ISO;ISSM/ISSO; - Verizon SCA – GSA or Independent Contractor | Security Authorization Package; artifacts include: SSP, SAR, POA&M, RAR, and Continuous Monitoring Plan. |
| **Task 5-3**—Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. | AO or Designated Representative - GSA | N/A |
| **Task 5-4**—Determine if risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable. | AO - GSA | Authorization decision document (e.g. ATO, DATO, etc.) |

**TASK 5-1: Plan of Action and Milestones (POA&M).** Following assessment of the information system in RMF Step Four, the POA&M is prepared and/or updated based on the results of the security assessment and any remedial action to correct findings. The POA&M includes vulnerabilities (except those identified as ''Mitigated' or 'Resolved') in the information system documented in SAR. The POA&M also describes how the Information System Owner intends to address those vulnerabilities (i.e., reduce, eliminate, or accept vulnerabilities). Verizon will develop the POA&M in accordance with GSA IT Security Procedural Guide 09-44, Plan of Action and Milestones (POA&M) using the GSA provided template. Verizon is responsible for implementing and administering an Information Security program to protect its information resources, in compliance with applicable laws, regulations, and corporate policies. Verizon's IT Governance Risk and Compliance (GRC) groups have created the Information Security POA&M Guide to provides consistency around the POA&M process. Consistent with industry practice, Verizon leverages a POA&M management process to:

- Plan and monitor corrective actions;
- Define roles and responsibilities for weakness resolution;
- Help identify the security funding requirements necessary to mitigate weaknesses;
- Track and prioritize resources; and
- Inform decision makers.

Weakness remediation is the process whereby security vulnerabilities are identified, corrective actions are initiated, and the weaknesses are properly mitigated.

**Note:** For Open or Outstanding findings in the Security Assessment Report, there will be a related planned action in the POA&M and in the System Security Plan for that NIST 800-53 control or enhancement.

**TASK 5-2: Security Authorization Package.** Once the BSS POA&M is completed, Verizon will update the SSP to reflect the results of the security assessment and any modifications to the security controls in the information system. When completed, the SSP reflects the actual state of the security controls implemented in the system following completion of security assessment activities. This is necessary to account for any modifications made to address recommendations for corrective actions from the security assessor. Verizon will also update the GSA NIST 800-53 R4 Control Tailoring Workbook, Control Implementation Summary Table, and other security-related appendices to the SSP. During this task, the Security Authorization Package is assembled and includes the documents identified in **Table 8.6.6-2**.

**Table 8.6.6-2. Security Authorization Documentation.**

| POA&M Advantages | |
|---|---|
| ▪ Independent Penetration Test Report | ▪ Code Review Report |
| ▪ Interconnection Agreements (as applicable) | ▪ Contingency Plan |
| ▪ NIST SP 800-53 R4 Control Tailoring Workbook | ▪ Rules of Behavior |
| ▪ Incident Response Test Report | ▪ Certification Letter |
| ▪ Configuration Management Plan | ▪ Authorization Letter |
| ▪ Contingency Plan Test Report | ▪ Incident Response Plan |
| ▪ Required Policies and Procedures | ▪ System Security Plan |
| ▪ Control Implementation Summary | ▪ POA&M |
| ▪ Privacy Threshold Analysis/Privacy Impact Assessment | ▪ Continuous Monitoring Plan |
| ▪ Security/Risk Assessment Report (with required appendices) | |

Upon completion, Verizon submits the Security Authorization Package to the GSA OSAISO who will review the package using the OSAISO Security Authorization Package Review Standard Operating Procedure (SOP) guide. The SOP documents the

process for submission of security authorization packages to the OSAISO and the detailed procedural steps performed by the OSAISO to verify security authorization package compliance. Upon OSAISO concurrence, the package will be submitted to the GSA AO for adjudication. The security authorization package provides the authorizing official the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

**TASK 5-3: Risk Determination.** As part of the security authorization process, the GSA AO reviews the Security Authorization package to determine if vulnerabilities identified in the information system pose an acceptable level of risk to customer agency operations, assets, and individuals before granting an authorization decision. The explicit acceptance of risk is the responsibility of the GSA AO and customer organizations. The GSA AO and customer must consider many factors, balancing security considerations with mission and operational needs. The GSA AO issues an authorization decision for the information system after reviewing the authorization package submitted by the System Owner. The authorization package provides the GSA AO and customers with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system.

**TASK 5-4: Risk Acceptance.** If for any valid, operational reason, Verizon is unable to comply with a specific authoritative security policy (e.g., FISMA/NIST), standard, or security requirement and is unable to fully remediate the issue through the Plan of Action and Milestones process, it may request risk acceptance through approved organizational channels as specified by the GSA AO. However, compensating controls must be put in place to mitigate the risk level and these must be fully documented and demonstrated to effectively mitigate the risk. Following review of the security authorization package and consultation with key Agency officials, the GSA AO must render an authorization decision to accomplish the tasks identified in **Table 8.6.6-3**.

**Table A.6.6-3. Risk Mitigation Authorization Decision.**

| Risk Mitigation Authorization Decision |
|---|
| ▪ Authorize system operation without any restrictions or limitations on it operation. |
| ▪ Authorize system operation with restriction or limitation on its operation. The POA&M must include detailed corrective actions to correct deficiencies. Resubmit an updated authorization package upon completion of required POA&M actions to move to authorization to operate w/out any restrictions The POA&M will include detailed corrective actions to correct deficiencies. Resubmit an updated authorization package upon completion of required POA&M actions to move to |

| Risk Mitigation Authorization Decision |
|---|
| authorization to operate without any restrictions.<br>▪ Not authorized for operation. |

Upon receipt of the GSA AO authorization decision, Verizon will update the SSP and POA&M to reflect conditions (if any) set forth in the authorization decision letter.

### 8.6.7 RMF Step Six – Monitor Security Controls

Upon receipt of an ATO issued by a GSA AO, the sixth and final step of the Verizon BSS RMF process is to monitor the security controls. Using NIST SP 800-137 and GSA IT Security Procedural Guide CIO-IT Security-12-66 as guidance, Verizon will establish a continuous monitoring program that evaluates the implementation and operation of the security controls within the BSS system boundary. The overall focus of the BSS continuous monitoring program is to provide adequate information about security control effectiveness and organizational security status, thereby allowing the AO to make informed, timely security risk management decisions aimed at supporting the system authorization. The Verizon BSS continuous monitoring program leverages both manual and automated processes. Technical security controls are monitored using automated tools; manual monitoring is conducted for controls that cannot be automated or are not easily automatable. This strategy ensures that key information security controls, including management and operational controls, are periodically assessed for effectiveness.

Key elements of the Verizon Continuous Monitoring program are configuration management, system and security control monitoring, system status reporting, and documentation updates. NIST SP 800-37 outlines the seven tasks necessary for the implementation of an effective continuous monitoring program. **Table 8.6.7-1** outlines the seven supporting tasks, identifies the person or role responsible for each task, and specifies the deliverables associated with those tasks for Step Six—Monitor Security Controls.

**Table 8.6.7-1. RMF Step Six – Monitor Security Controls.**

| Supporting Tasks | Primary Responsibility | Deliverables |
|---|---|---|
| **Task 6-1.** Determine the security impact of proposed or actual changes to the IS and its environment of operation. | ISO or CCP;<br>ISSO/ ISSM – Verizon | Change Request |
| **Task 6-2.** Assess a selected subset of security controls employed within and inherited by the IS in accordance with the organization-defined monitoring strategy. | SCA; – GSA or Independent Contractor<br>ISSO/ ISSM – Verizon | Periodic Continuous Monitoring Report |

| Supporting Tasks | Primary Responsibility | Deliverables |
|---|---|---|
| **Task 6-3.** Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the POA&M. | ISO or CCP; ISSM/ISSO – Verizon | Documented evidence of correction (e.g., scan results, registry "dumps,"). |
| **Task 6-4.** Update the SSP, SAR, and POA&M based on the results of the continuous monitoring process. | ISO or CCP – Verizon | SSP, SAR, , and POA&M |
| **Task 6-5.** Report the security status of the IS (including the effectiveness of security controls employed within and inherited by the IS) to the AO and other appropriate organizational officials on an ongoing basis, in accordance with the Monitoring Strategy. | ISO or CCP – Verizon | Periodic Continuous Monitoring Report |
| **Task 6-6.** Review the reported security status of the IS (including the effectiveness of security controls employed within and inherited by the IS) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable. | AO – GSA | ATO |
| **Task 6-7.** Implement an IS Decommissioning Strategy, as needed, to execute required actions when a system is removed from service. | ISO – Verizon | Updated system inventory |

**TASK 6-1: Determine Security Impact of Changes.** OMB Circular A-130 requires that the security controls in each system be reviewed when significant modifications are made to the system, or at least every three years. In compliance with the concept of ongoing authorization and in compliance with FISMA, Verizon will work with the GSA AO to update the security authorization as needed, based on changes to the information system or at least every three years, or when there is a significant change as defined in NIST SP 800-37. **Table 8.6.7-2** identifies changes to the BSS system or environment of the operations may also require a reauthorization:

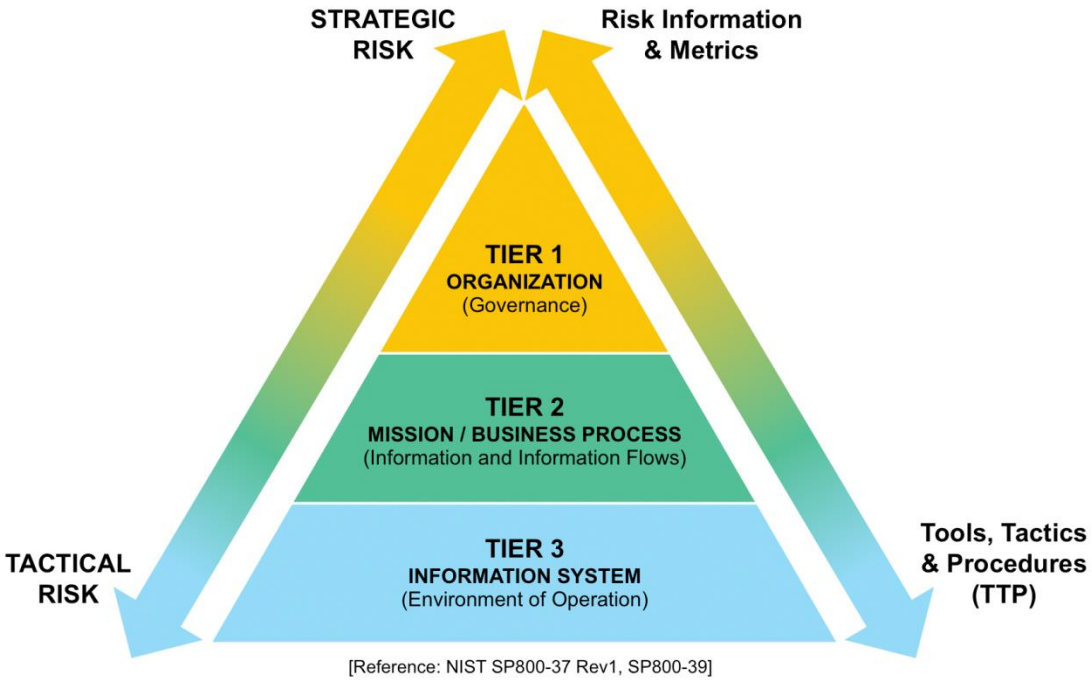
**Table 8.6.7-2. EIS IT System Security Impact Changes.**

| EIS IT System Security Impact Changes |
|---|
| ▪ Addition or replacement of a major component or part of a major system |
| ▪ A change in security mode of operation |
| ▪ A change in interfacing systems |
| ▪ A significant change to the operating system or executive software |
| ▪ A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the authorization |
| ▪ A significant change to the physical structure housing the information system or environment of the information system that could affect the physical security described in the authorization |
| ▪ A significant change to the threat that could adversely affect the systems |
| ▪ A significant change to the availability of safeguards |
| ▪ A significant change to the user population |

**TASK 6-2: Assess Security Control Implementation.** As shown in **Figure 8.6.7-1**, a robust and comprehensive continuous monitoring strategy is fully integrated within Verizon's system development life cycle process to promote risk management on an

ongoing basis and will significantly reduce the resources required for re-authorization. Using automation, state of the art practice, techniques, and procedures, risk management can be accomplished in near real-time along with the ongoing monitoring of security controls and changes to the information system and its operational environment.

**Figure 8.6.7-1. Verizon RMF and ISCM Alignment.**




Effective continuous monitoring is conducted in accordance with the specified requirements of the authorizing official and results in the production of key information that is essential for determining: (i) the current security state of the information system (including the effectiveness of the security controls employed within and inherited by the system); (ii) the resulting risks to organizational operations, organizational assets, individuals, other organizations and the nation; and (iii) effective authorization decisions that reveal the state of both the fully implemented and inherited controls. Verizon Federal Information Systems and solutions are continuously monitored and assessed. To confirm accuracy in tracking compliance with the controls, the compliance team conducts quarterly attestations with each system owner. System owners are further asked to review control language for accuracy and clarity. Upon completion, each system owner must attest to the fact that they are in full compliance with the control

requirement. Any identified gap or deficiency must be promptly reported and a corrective action plan (CAP) must be established. CAPs are subsequently tracked and reported within the POA&M reporting process.

**TASK 6-3: Conduct Remediation Actions.** Verizon, as part of its Continuous Monitoring program, remediates identified security issues. As discussed in RMF Task 4-4 above, Verizon continually conducts security control remediation efforts based on the CAPs created in RMF Task 6-2 and reassesses remediated control(s), as appropriate. The Verizon ISSO will manage the remediation efforts by leveraging Verizon's Plan of Action and Milestone (POA&M) process. If a critical/high vulnerability is discovered, it must either be remediated or have the severity level reduced to a medium or low within 30 days. Moderate vulnerabilities must be remediated or have the severity level reduce to a low within 90 days.

**TASK 6-4: Update Security Documentation.** Throughout RMF Step Six, the documents created in previous steps, as well as the system inventory, are updated as required. POA&Ms are updated monthly. Other security documents (e.g., SSP, SAR, and other security-related plans) are updated as required but at least annually, as part routine configuration management and monitoring activities.

**TASK 6-5: Report Security Status on an On-Going Basis.** The security state of BSS will be reported to the GSA by Verizon, as required by the EIS RFP. Verizon is working to implement a fully automated continuous monitoring architecture as specified in the GSA IT Security Procedural Guide CIO-IT Security-12-66, Information Security Continuous Monitoring Strategy.

**TASK 6-6: Risk Determination.** As discussed in RMF Task 5-3 above, Verizon will provide the GSA AO with the essential information (including the effectiveness of security controls employed within and inherited by the IS) on an ongoing basis in accordance with the monitoring strategy. This allows the GSA AO to determine whether there is acceptable risk to organizational operations, organizational assets, individuals, other organizations, or the United States as a whole.

**TASK 6-7: Implement Decommissioning Strategy.** When a Verizon information system is removed from operation, a number of risk management-related actions are required. Verizon confirms that security controls addressing information system removal and disposal are implemented (e.g., media sanitization, configuration management and control). Asset inventory tracking and management systems are updated to indicate the specific information system components that are being removed from service. Security status reports are updated to reflect the new status of the information system. Users and application owners hosted on the decommissioned information system are notified as appropriate, and any security control inheritance relationships are reviewed and assessed by Verizon for impact. This task also applies to subsystems that are removed or decommissioned. Verizon assesses the effects of the subsystem removal or disposal with respect to the overall operation of the information system where the subsystem resided, or in the case of dynamic subsystems, the information systems where the subsystems were actively employed.

## 8.7 Key BSS Security Deliverables

As specified in RFP Section G.5.6.4, Verizon will create, maintain and update the security A&A documentation identified in **Table 8.7-1** below, for the BSS offering:

**Table 8.7-1. Key Verizon BSS Security Deliverables.**

| Verizon BSS Security Deliverables |
|---|
| **System Security Plan (SSP).** The BSS SSP will be completed in accordance NIST SP 800-18 and other relevant guidelines. The SSP will include, at a minimum, a narrative and appendices containing the required policies, procedures and supporting artifacts across the NIST SP 800-53 security control families mandated per FIPS 200. As appropriate, the remaining documents in this table will be included in the SSP. |
| **Security Assessment Boundary and Scope Document (BSD).** This document defines the actual security assessment boundary as identified in NIST SP 800-37. |
| **Interconnection Security Agreements (ISA).** The ISAs document interconnections with other systems in accordance with NIST SP 800-47. (Reference: NIST SP 800-53 R4: CA-3). |
| **GSA NIST SP 800-53 R4 Control Tailoring Workbook.** This workbook documents contractor-implemented settings that are different from GSA-defined settings, and where GSA-defined settings allow a contractor to deviate, as identified in GSA IT Security Procedural Guide CIO-IT Security-06-30. |
| **GSA NIST SP 800-53 R4 Control Summary Table for a Moderate Impact Baseline.** This document defines the implementation status of each NIST SP 800-53 R4 security control and enhancement as identified in GSA IT Security Procedural Guide CIO-IT Security-06-30. |
| **Rules of Behavior (RoB).** The RoB defines the rules that must be followed by information system users as identified in GSA IT Security Procedural Guide CIO-IT Security-06-30 and GSA Order CIO 2104.1. (Reference: NIST SP 800-53 R4: PL-4). |
| **System Inventory.** The system inventory includes hardware, software and related information as identified in GSA IT Security Procedural Guide CIO-IT Security-06-30. |
| **Contingency Plan (CP).** The Contingency Plan includes a Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) in agreement with NIST SP 800-34. (Reference: NIST SP 800-53 R4: CP-2). |
| **Contingency Plan Test Plan (CPTP).** The CPTP will be completed in agreement with GSA IT Security Procedural Guide CIO-IT Security-06-29. (Reference: NIST SP 800-53 R4: CP-4). |
| **Contingency Plan Test Report (CPTR).** The CPTR documents the result of the CP test conducted using the CPTP |

| Verizon BSS Security Deliverables |
|---|
| in agreement with GSA IT Security Procedural Guide CIO-IT Security-06-29. (Reference: NIST SP 800-53 R4: CP-4). |
| **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA).** A Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) will be completed as identified in GSA IT Security Procedural Guide CIO-IT Security-06-30. (Reference: NIST SP 800-53 R4: AR-2, AR-3 and AR-4). |
| **Configuration Management Plan (CMP).** The CMP documents the process used to maintain the secure configuration of the system in agreement with NIST SP 800-128. The CMP will include the System Baseline Configuration Standard Document that provides a well-defined, documented, and up-to-date specification to which the information system is built. (Reference: NIST SP 800-53 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05) |
| **Incident Response Plan (IRP).** The IRP defines actions that will be taken in response to a computer security incident in accordance with NIST SP 800-61 (Reference: NIST 800-53 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02). |
| **Incident Response Test Report (IRTR).** The Response Test Report (IRTR) documents the results of the incident response plan test (Reference: NIST SP 800-53 controls IR-3 and IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02). |
| **System Configuration Settings.** The System Configuration Settings document the mandatory configuration settings for information technology products employed within the BSS that reflect the most restrictive mode consistent with operational requirements. BSS systems will be configured in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening systems, as deemed appropriate by the AO. (Reference: NIST SP 800-53 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05). |
| **Continuous Monitoring Plan.** The Continuous Monitoring Plan documents how continuous monitoring of information system will be accomplished. Through continuous monitoring, security controls and supporting deliverables will be updated and submitted to GSA. The submitted deliverables provide a current understanding of the security state and risk posture of the information systems. They allow GSA authorizing officials to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. (Reference: NIST SP 800-53 R4: CA-7). |
| **Plan of Action and Milestones (POA&M).** The Plan of Action and Milestones will be completed in agreement with GSA IT Security Procedural Guide 06-30. Scans associated with the POA&M will be performed as an authenticated user with elevated privileges. Vulnerability scanning results will be managed and mitigated in the POA&M and submitted together with the quarterly POA&M submission. (Reference: NIST SP 800-53 R4; RA-5, CA-5 and GSA CIO-IT Security Guide 06-30). |
| **Independent Penetration Test Report.** The Independent Penetration Test Report documents the results of vulnerability analysis and exploitability of identified vulnerabilities in accordance with GSA CIO-IT Security Guide 11-51. Penetration test exercises will be coordinated through the GSA Office of the Chief Information Security Officer (OCISO) Security Engineering (ISE). (Reference: NIST SP 800-53 R4: CA-5 and RA-5). |
| **Code Analysis Review Report.** The Code Analysis Report documents the results of code analysis reviews that will be conducted in accordance with GSA CIO Security Procedural Guide 12-66 using the appropriate automated tools (e.g., Fortify, Veracode) to examine for common flaws. (Reference: NIST SP 800-53, R4: SA-11; GSA CIO Security Procedural Guides 06-30; and GSA CIO Security Procedural Guide 12-66.) |
| **Security/Risk Assessment Report (SAR).** The Government is responsible for providing the Security/Risk Assessment Report. Identified gaps between required 800-53 controls and the Verizon's implementation as documented in the SAR will be tracked for mitigation in a POA&M document completed in accordance with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)." |
| **Annual FISMA Assessment.** Verizon will deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation". Each fiscal year the annual assessment will be completed in accordance with instructions provided by GSA (Reference: NIST SP 800-53 R4: CA-2). |
| **Information Security Policies and Procedures.** Verizon has developed and maintains policy and procedures documents in the Verizon Public Sector Information Security Program Plan, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides. These policies and procedures include:<br>o Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1)<br>o Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1)<br>o Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1)<br>o Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1)<br>o Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1)<br>o Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1)<br>o Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1)<br>o Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1)<br>o System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1) |

| Verizon BSS Security Deliverables |
| --- |
| ○ Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1)<br>○ Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1)<br>○ Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1)<br>○ Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1)<br>○ Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1)<br>○ Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1)<br>○ System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1)<br>○ System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1) |

Verizon will maintain and update these key BSS security deliverables in accordance with guidance provided by the NIST Special Publications and the Authorizing Official.