

Proposed Security  
Assessment & Authorization  
for U.S. Government Cloud Computing

---



---

Draft version 0.96  
November 2, 2010

# Preface

---

## **Proposed Security Assessment and Authorization for U.S. Government Cloud Computing:**

Over the past 18 months, an inter-agency team comprised of the National Institute of Standards and Technology (NIST), General Services Administration (GSA), the CIO Council and working bodies such as the Information Security and Identity Management Committee (ISIMC), has worked on developing the Proposed Security Assessment and Authorization for U.S. Government Cloud Computing. This team evaluated security controls and multiple Assessment and Authorization models for U.S. Government Cloud Computing as outlined in this document.

The attached document is a product of 18 months of collaboration with State and Local Governments, Private Sector, NGO's and Academia. This marks an early step toward our goal of deploying secure cloud computing services to improve performance and lower the cost of government operations, but we need to improve this document through your input.

Often stated, but still true, we recognize that we do not have a monopoly on the best ideas. We seek your input, knowledge, and experience to help us frame appropriate security controls and processes for the Federal Government's journey to cloud computing. The attached document is a draft and is designed to encourage robust debate on the best path forward.

Comments on the documents should be submitted online at [www.FedRAMP.gov](http://www.FedRAMP.gov) by December 2<sup>nd</sup>. We look forward to your active engagement and substantive comments.

Vivek Kundra  
U.S. Chief Information Officer

# To Submit Comments

---

Comments on the documents can be submitted using the FedRAMP online comment form available at [www.FedRAMP.gov](http://www.FedRAMP.gov) through 11:59 pm Eastern Time on December 2<sup>nd</sup>. Comments can be made either anonymously or by providing contact information, if attribution or follow up is requested. At the conclusion of the comment period, a joint tiger team of representatives from across government will review the comments for inclusion in the final documents.

**Press inquiries should be directed to Sara Merriam, GSA's Press Secretary, at 202-501-9139.**

The comment form asks for the following information:

- **Organization Type:** Please indicate whether you are reporting your comment as a member of government, industry, or the community-at-large.
- **Company or Agency Name:** This optional field will allow you to provide attribution to the agency or company that you work for.
- **Document Name:** To comment on this document, please select the first item in the list, “FedRAMP: Security Controls, Guidelines & Process for US Government Cloud Computing”. If commenting on the reference documents, please indicate to which reference document your comment relates.
- **Section Number:** Please indicate to which section number or section name your comment relates. Examples from this text would be “2. FedRAMP Security Controls”, “FedRAMP Security Controls” or “2”. This is meant to assist the review team in locating the context for your comment.
- **Page Number:** Please indicate the page number on which your comment relates. Page numbers are found at the bottom of each page in each document.
- **Line or Table Number:** Through the documents, the text has a line number on the left hand side of the page. Please reference the line number in question; or in the case of tables, the table's unique identifier in the left . Examples from this text would be “530” or “AC-1”.
- **Comment Type:** To facilitate review and action of the comments, please identify your comment into one of the following categories.
  - **Editorial** – The comment relates to the text's wording or formatting but does not impact the underlying content of the text.
  - **Policy** – The comment relates to specific government policy or a requested change thereto.
  - **Procedural** – The comment relates to the proposed process by which FedRAMP will conduct operations.
  - **Question** – The comment is a question about either the intent or interpretation of the text. It is anticipated that an FAQ document will be drafted as a result of questions received.
  - **Technical** – The comment relates to either the technical implementation of a control, assessment procedure, template or process in one of the documents.
  - **Other** – If your comment doesn't fit into one of the other categories, please use this categorization.
- **Visibility** – Either Public if the comment or its resulting answer should be posted to the general public or if a response should only be sent to the specific commentator. If private, please include contact information.
- **Comment** – Please enter your comment here.
- **Proposed Resolution** – If your comment relates to a change, please identify your suggested resolution within this field.
- **Contact Information** – If you would like a direct response to your comment, please include contact information in the form of your name and email address. Please note that all contact information will be kept confidential.

# Document Organization & Reference Material

---

This document describes the U.S. Government's proposed Assessment and Authorization (A&A) for U.S. Government Cloud Computing. The document is organized in to three Chapters, each chapter details a necessary element in creating a framework from which a government-wide A&A could function. The three chapters are as follows:

## **Chapter 1: Cloud Computing Security Requirement Baseline**

This chapter presents a list of baseline security controls for Low and Moderate impact Cloud systems. NIST Special Publication 800-53R3 provided the foundation for the development of these security controls.

## **Chapter 2: Continuous Monitoring**

This chapter describes the process under which authorized cloud computing systems will be monitored. This section defines continuous monitoring deliverables, reporting frequency and responsibility for cloud service provider compliance with FISMA.

## **Chapter 3: Potential Assessment & Authorization Approach**

This chapter describes the proposed operational approach for A&A's for cloud computing systems. This reflects upon all aspects of an authorization (including sponsorship, leveraging, maintenance and continuous monitoring), a joint authorization process, and roles and responsibilities for Federal agencies and Cloud Service Providers in accordance with the Risk Management Framework detailed in NIST Special Publication 800-37R1.

## **Reference Material**

In addition to the three chapters detailed above, the following artifacts are also available as reference material:

- **Assessment Procedures**  
The assessment procedures are intended to be used by independent 3rd party assessors in their review of cloud service provider systems and the corresponding development of the security assessment, risk assessment reports.
- **Security Documentation Templates**  
The templates required for completing all the artifacts for assessment & authorization are available as reference material. Cloud Service Providers can use the templates to develop and submit artifacts for assessment & authorization.

# Acronym Definitions

---

<b>Term</b>	<b>Definition</b>
<b>A&amp;A</b>	Assessment and Authorization
<b>AC</b>	Access Control
<b>ASHRAE</b>	American Society of Heating, Refrigerating and Air-conditioning Engineers
<b>AT</b>	Awareness and Training
<b>ATO</b>	Authority to Operate
<b>AU</b>	Audit and Accountability
<b>CA</b>	Assessment and Authorization
<b>CCP</b>	Configuration Change Control process
<b>CIS</b>	Center for Internet Security
<b>CM</b>	Configuration Management
<b>CMP</b>	Continuous Monitoring Plan
<b>CP</b>	Contingency Planning
<b>CSP</b>	Cloud Service Provider
<b>FCCI</b>	Federal Cloud Computing Initiative
<b>FDCC</b>	Federal Desktop Core Configuration
<b>FedRAMP</b>	Federal Risk and Authorization Management Program
<b>FIPS</b>	Federal Information Processing Standard
<b>FISMA</b>	Federal Information Security Management Act
<b>IA</b>	Identification and Authentication
<b>ICAM</b>	Identity, Credential and Access Management
<b>IR</b>	Incident Response
<b>ISIMC</b>	Information Security and Identity Management Committee
<b>IV&amp;V</b>	Independent Validation & Verification
<b>JAB</b>	Joint Authorization Board
<b>MA</b>	Maintenance
<b>MP</b>	Media Protection
<b>NIST</b>	National Institute of Standards & Technology
<b>PE</b>	Physical and Environmental Protection
<b>PIA</b>	Privacy Impact Assessment
<b>PL</b>	Planning

<b>Term</b>	<b>Definition</b>
<b>POA&amp;M</b>	Plan of Action & Milestones
<b>POSV</b>	Proprietary Operating System Vendor
<b>PS</b>	Personnel Security
<b>RA</b>	Risk Assessment
<b>RMF</b>	Risk Management Framework
<b>SA</b>	System and Services Acquisition
<b>SAR</b>	Security Assessment Report
<b>SC</b>	System and Communications Protection
<b>SCAP</b>	Security Content Automation Protocol
<b>SDLC</b>	System Development Life Cycle
<b>SI</b>	System and Information Integrity
<b>SSP</b>	System Security Plan
<b>TIC</b>	Trusted Internet Connection
<b>USGCB</b>	United States Government Configuration Baseline

# Table of Contents

---

Chapter One: Cloud Computing Security Requirements Baseline .....	1
1.1. Access Control (AC) .....	3
1.2. Awareness and Training (AT) .....	6
1.3. Audit and Accountability (AU) .....	7
1.4. Assessment and Authorization (CA) .....	10
1.5. Configuration Management (CM) .....	11
1.6. Contingency Planning (CP) .....	13
1.7. Identification and Authentication (IA) .....	15
1.8. Incident Response (IR) .....	18
1.9. Maintenance (MA) .....	19
1.10. Media Protection (MP) .....	20
1.11. Physical and Environmental Protection (PE) .....	21
1.12. Planning (PL) .....	23
1.13. Personnel Security (PS) .....	24
1.14. Risk Assessment (RA) .....	25
1.15. System and Services Acquisition (SA) .....	26
1.16. System and Communications Protection (SC) .....	27
1.17. System and Information Integrity (SI) .....	31
Chapter Two: Continuous Monitoring .....	35
2.1. Introduction .....	36
2.2. Purpose .....	36
2.3. Background .....	36
2.4. Continuous Monitoring Requirements .....	37
2.5. Reporting and Continuous Monitoring .....	37
2.6. Routine Systems Change Control Process .....	39
2.7. FISMA Reporting Requirements .....	39
2.8. On-going Testing of Controls and Changes to Security Controls Process .....	40
2.9. Incident Response .....	41
2.10. Independent Verification and Validation .....	43
Chapter Three: Potential Assessment & Authorization Approach .....	45
3.1. Introduction .....	46
3.2. Overview .....	47
3.3. Governance .....	48
3.4. Assessment and Authorization Processes .....	52
3.5. Authorization Maintenance Process .....	70
3.6. Authorization Leveraging Process .....	71
3.7. Communications Process .....	72
3.8. Change Management Process .....	78

## 1 Executive Overview

2 The ability to embrace cloud computing capabilities for federal departments and agencies brings  
3 advantages and opportunities for increased efficiencies, cost savings, and green computing  
4 technologies. However, cloud computing also brings new risks and challenges to securely use  
5 cloud computing capabilities as good stewards of government data. In order to address these  
6 concerns, the U.S. Chief Information Officer (U.S. CIO) requested the Federal CIO Council  
7 launch a government-wide risk and authorization management program. This document  
8 describes a government-wide Federal Risk and Authorization Management Program (FedRAMP)  
9 to provide joint security assessment, authorizations and continuous monitoring of cloud  
10 computing services for all Federal Agencies to leverage.

11 Cloud computing is not a single capability, but a collection of essential characteristics that are  
12 manifested through various types of technology deployment and service models. A wide range of  
13 technologies fall under the title “cloud computing,” and the complexity of their various  
14 implementations may result in confusion among program managers. The guidelines embraced in  
15 this document, represent a subset of the National Institute of Standards and Technology (NIST)  
16 definition of cloud computing, with three service models; Software as a Service, Platform as a  
17 Service, and Infrastructure as a Service (SaaS, PaaS, and IaaS).

18 The decision to embrace cloud computing technology is a risk-based decision, not a technology-  
19 based decision. As such, this decision from a risk management perspective requires inputs from  
20 all stakeholders, including the CIO, CISO, Office of General Counsel (OGC), privacy official  
21 and the program owner. Once the business decision has been made to move towards a cloud  
22 computing environment, agencies must then determine the appropriate manner for their security  
23 assessments and authorizations.

## 24 CLOUD COMPUTING AND GOVERNMENT-WIDE RISK AND AUTHORIZATION

25 Cloud Computing systems are hosted on large, multi-tenant infrastructures. This shared  
26 infrastructure provides the same boundaries and security protocols for each customer. In such an  
27 environment, completing the security assessment and authorization process separately by each  
28 customer is redundant. Instead, a government-wide risk and authorization program would enable  
29 providers and the program office to complete the security assessment and authorization process  
30 once and share the results with customer agencies.

31 Additionally, the Federal Information Security Management Act (FISMA) and NIST special  
32 publications provide Federal Agencies with guidance and framework needed to securely use  
33 cloud systems. However, interpretation and application of FISMA requirements and NIST  
34 Standards vary greatly from agency to agency. Not only do agencies have varying numbers of  
35 security requirements at or above the NIST baseline, many times additional requirements from  
36 multiple agencies are not compatible on the same system. A government-wide risk and  
37 authorization program for cloud computing would allow agencies to completely leverage the  
38 work of an already completed authorization or only require an agency to complete delta  
39 requirements (i.e. unique requirements for that individual agency).

40 Finally, security authorizations have become increasingly time-consuming and costly both for  
41 the Federal Government and private industry. As depicted in Figure 1, government-wide risk and

42 authorization program will promote faster and cost-  
43 effective acquisition of cloud computing systems by  
44 using an ‘authorize once, use many’ approach to  
45 leveraging security authorizations. Additionally,  
46 such a program will promote the Administration’s  
47 goal of openness and transparency in government.  
48 All of the security requirements, processes, and  
49 templates will have to be made publicly available  
50 for consumption not only by Federal agencies but  
51 private vendors as well. This will allow Federal  
52 Agencies to leverage this work at their agency but private industry will also finally have the full  
53 picture of what a security authorization will entail prior to being in a contractual relationship  
54 with an agency.

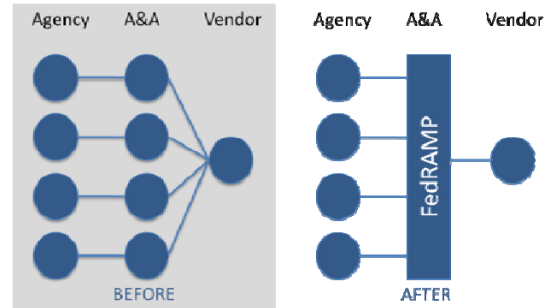


Figure 1: FedRAMP eliminates redundancy.

## 55 **STANDARDIZED ASSESSMENT & AUTHORIZATION: FedRAMP**

56 The Federal Risk and Authorization Management Program (FedRAMP) is designed to solve the  
57 security authorization problems highlighted by cloud computing. FedRAMP will provide a  
58 unified government-wide risk management process for cloud computing systems. FedRAMP will  
59 work in an open and transparent manner with Federal Agencies and private industry about the  
60 Assessment and Authorization process.

61 Through this government-wide approach, FedRAMP will enable agencies to either use or  
62 leverage authorizations with an:

- 63 • Interagency vetted approach using common security requirements;
- 64 • Consistent application of Federal security requirements;
- 65 • Consolidated risk management; and
- 66 • Increased effectiveness and management cost savings.

67 In addition, FedRAMP will work in collaboration with the CIO Council and Information  
68 Security and Identity Management Committee (ISIMC) to constantly refine and keep this  
69 document up to date with cloud computing security best practices. Separate from FedRAMP,  
70 ISIMC has developed guidance for agency use on the secure use of cloud computing in *Federal*  
71 *Security Guidelines for Cloud Computing*.

## 72 **TRANSPARENT PATH FOR SECURE ADOPTION OF CLOUD COMPUTING**

73 The security guidance and FedRAMP assessment and authorization process aims to develop  
74 robust cloud security governance for the Federal Government. The collective work that follows  
75 represents collaboration amongst security experts and representatives throughout government  
76 including all of the CIO Council Agencies.

77 By following the requirements and processes in this document, Federal agencies will be able to  
78 take advantage of cloud based solutions to provide more efficient and secure IT solutions when  
79 delivering products and services to its customers.

# Chapter One: Cloud Computing Security Requirements Baseline

## 80 1. Cloud Computing Security Requirements Baseline

81 This chapter identifies (by security control number and name) the security controls from NIST  
82 Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal*  
83 *Information Systems and Organizations* (as amended). These controls have been agreed to by a  
84 Joint Approval Board made up of users from GSA, DHS & DOD for use within information  
85 systems providing cloud computing services to the Federal government.

86 The security controls contained in this publication work in concert with NIST Special  
87 Publication 800-53, Revision 3. Table 1 (begins on page 3) specifies control parameter  
88 definitions and additional requirements or guidance in addition to NIST Special Publication 800-  
89 53, Revision 3 for a FedRAMP A&A package. NIST Special Publication 800-53, Revision 3  
90 details security controls that apply to all federal information systems, and authorizing officials  
91 and information system owners have the authority and responsibility to develop security plans  
92 which define how the controls are implemented within their particular information systems and  
93 environments of operation.

94 In the case of FedRAMP, two sets of security controls have been defined for low-impact and  
95 moderate-impact cloud information systems respectively. The impact levels are based on the  
96 sensitivity and criticality of the federal information being processed, stored, and transmitted by  
97 cloud information systems as defined in Federal Information Processing Standard 199. All NIST  
98 security standards and guidelines used to define the requirements for the FedRAMP cloud  
99 computing initiative are publicly available at <http://csrc.nist.gov>.

100 The FedRAMP defined security controls are presented in Table 1: FedRAMP Security Controls.  
101 This table is organized by the 17 control families identified in NIST Special Publication 800-53,  
102 Revision 3. The table presents the following information:

- 103 • **Control Number and Name** – The control number and control name relate to the control  
104 as defined in NIST Special Publication 800-53, Revision 3.
- 105 • **Control Baseline** – The control is listed in either the Low or Moderate impact column  
106 where applicable to that baseline. If the control is not applicable, a blank will appear in  
107 that column. If a control enhancement is applicable, the enhancement is designated  
108 inside of parenthesis. Additional security controls and control enhancements that are  
109 not included in the low and moderate control baselines defined in NIST Special  
110 Publication 800-53 Revision 3 (Appendix D) are denoted in **bold** font. For example,  
111 AC-2 : Control is included in the NIST Baseline  
112 AC-2 (1) : Control enhancement is included in the NIST Baseline  
113 **AC-2 (7)** : FedRAMP specific control enhancement.
- 114 • **Control Parameter Requirements** – Certain controls are defined with implementation  
115 parameters. These parameters identify the scope, frequency and other considerations for  
116 how cloud service providers address specific controls and enhancements.
- 117 • **Additional Requirements & Guidance** – These entries represent additional required  
118 security controls for cloud computing applications and environments of operation  
119 selected from the security control catalog in NIST Special Publication 800-53 Revision 3  
120 (Appendix F). Required parameter *values* for the variable parts of security controls and  
121 control enhancements (designated by *assignment* and *selection* statements) are also  
122 provided.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
<b>1.1. Access Control (AC)</b>					
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
AC-2	Account Management	AC-2	AC-2 AC-2 (1) AC-2 (2) AC-2 (3) AC-2 (4) <b>AC-2 (7)</b>	AC-2j. [Assignment: organization-defined frequency] Parameter: [at least annually]  AC-2 (2) [Assignment: organization-defined time period for each type of account (temporary and emergency)] Parameter: [no more than ninety days for temporary and emergency account types]  AC-2 (3) [Assignment: organization-defined time period] Parameter: [ninety days for user accounts] See additional requirements and guidance.	AC-2 (3) Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB.
AC-3	Access Enforcement	AC-3	AC-3 <b>AC-3 (3)</b>	AC-3 (3) [Assignment: organization-defined nondiscretionary access control policies] Parameter: [role-based access control]  [Assignment: organization-defined set of users and resources] Parameter: [all users and resources]	<b>AC-3 (3)</b> Requirement: The service provider: a. Assigns user accounts and authenticators in accordance within service provider's role-based access control policies; b. Configures the information system to request user ID and authenticator prior to system access; and 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.
AC-4	Information Flow Enforcement	Not Selected	AC-4	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AC-5	Separation of Duties	Not Selected	AC-5	None.	None.
AC-6	Least Privilege	Not Selected	AC-6 AC-6 (1) AC-6 (2)	<p>AC-6 (1) [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware and security-relevant information)] Parameter: See additional requirements and guidance.</p> <p>AC-6 (2) [Assignment: organization-defined list of security functions or security-relevant information] Parameter: [all security functions]</p>	<p>AC-6 (1) Requirement: The service provider defines the list of security functions. The list of functions is approved and accepted by the JAB.</p> <p>AC-6 (2) Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.</p>
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	<p>AC-7a. [Assignment: organization-defined number] Parameter: [not more than three]</p> <p>AC-7a. [Assignment: organization-defined time period] Parameter: [fifteen minutes]</p> <p>AC-7b. [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] Parameter: [locks the account/node for thirty minutes]</p>	None.
AC-8	System Use Notification	AC-8	AC-8	None.	None.
AC-10	Concurrent Session Control	Not Selected	<b>AC-10</b>	<p>AC-10 [Assignment: organization-defined number] Parameter: [one session]</p>	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AC-11	Session Lock	Not Selected	AC-11 <b>AC-11 (1)</b>	AC-11a. [Assignment: organization-defined time period] Parameter: [fifteen minutes]	None.
AC-14	Permitted Actions Without Identification/ Authentication	AC-14	AC-14 AC-14 (1)	None.	None.
AC-16	Security Attributes	Not Selected	<b>AC-16</b>	<b>AC-16</b> Assignment: organization-defined security attributes] Parameter: See additional requirements and guidance.	<b>AC-16</b> Requirement: The service provider defines the security attributes. The security attributes need to be approved and accepted by JAB.
AC-17	Remote Access	AC-17	AC-17 AC-17 (1) AC-17 (2) AC-17 (3) AC-17 (4) AC-17 (5) AC-17 (7) AC-17 (8)	AC-17 (5) [Assignment: organization-defined frequency] Parameter: [continuously, real time]  AC-17 (7) [Assignment: organization-defined list of security functions and security-relevant information] Parameter: See additional requirements and guidance.  AC-17 (8) [Assignment: organization-defined networking protocols within the information system deemed to be non-secure] Parameter: [fttp, (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]	AC-17 (7) Requirement: The service provider defines the list of security functions and security relevant information. Security functions and the implementation of such functions are approved and accepted by the JAB.  Guidance: Security functions include but are not limited to: establishing system accounts; configuring access authorizations; performing system administration functions; and auditing system events or accessing event logs; SSH, and VPN.  AC-17 (8) Requirement: Networking protocols implemented by the service provider are approved and accepted by JAB.  Guidance: Exceptions to restricted networking protocols are granted for explicitly identified information system components in support of specific operational requirements.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AC-18	Wireless Access	AC-18	AC-18 AC-18 (1) <b>AC-18 (2)</b> <b>AC-18 (3)</b> <b>AC-18 (4)</b> <b>AC-18 (5)</b>	<b>AC-18 (2)</b> [Assignment: organization-defined frequency] Parameter: [at least quarterly]	None.
AC-19	Access Control for Mobile Devices	AC-19	AC-19 AC-19 (1) AC-19 (2) AC-19 (3)	AC-19g. [Assignment: organization-defined inspection and preventative measures] Parameter: See additional requirements and guidance.	AC-19g. Requirement: The service provider defines inspection and preventative measures. The measures are approved and accepted by JAB.
AC-20	Use of External Information Systems	AC-20	AC-20 AC-20 (1) AC-20 (2)	None.	None.
<b>AC-21</b>	<b>User-Based Collaboration and Information Sharing</b>	Not Selected	<b>AC-21</b>	<b>AC-21a.</b> [Assignment: organization-defined information sharing circumstances where user discretion is required] Parameter: See additional requirements and guidance.  <b>AC-21b.</b> [Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required] Parameter: See additional requirements and guidance.	<b>AC-21a.</b> Requirement: The service consumer defines information sharing circumstances where user discretion is required.  <b>AC-21b.</b> Requirement: The service provider defines the mechanisms or manual processes for the information sharing circumstances defined by the service consumer.
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22d. [Assignment: organization-defined frequency] Parameter: [at least quarterly]	None.
<b>1.2. Awareness and Training (AT)</b>					
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
AT-2	Security Awareness	AT-2	AT-2	AT-2 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AT-3	Security Training	AT-3	AT-3	AT-3 [Assignment: organization-defined frequency] Parameter: [at least every three years]	None.
AT-4	Security Training Records	AT-4	AT-4	AT-4b. [Assignment: organization-defined frequency] Parameter: [At least three years]	None.
AT-5	Contacts With Security Groups and Associations	Not Selected	<b>AT-5</b>	None	None.
<b>1.3. Audit and Accountability (AU)</b>					
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AU-2	Auditable Events	AU-2	AU-2 AU-2 (3) AU-2 (4)	<p>AU-2a. [Assignment: organization-defined list of auditable events] Parameter: [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]</p> <p>AU-2d. [Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited] Parameter: See additional requirements and guidance.</p> <p>AU-2d. [Assignment: organization-defined frequency of (or situation requiring) auditing for each identified event]. Parameter: [continually]</p> <p>AU-2 (3) [Assignment: organization-defined frequency] Parameter: [annually or whenever there is a change in the threat environment]</p>	<p>AU-2d. Requirement: The service provider defines the subset of auditable events from AU-2a to be audited. The events to be audited are approved and accepted by JAB.</p> <p>AU-2 (3) Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB.</p> <p>AU-2 Requirement: 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.</p>
AU-3	Content of Audit Records	AU-3	AU-3 AU-3 (1)	<p>AU-3 (1) [Assignment: organization-defined additional, more detailed information] Parameter: [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]</p>	<p>AU-3 (1) Requirement: The service provider defines audit record types. The audit record types are approved and accepted by the JAB.</p> <p>Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.</p>
AU-4	Audit Storage Capacity	AU-4	AU-4	None.	None.
AU-5	Response to Audit Processing Failures	AU-5	AU-5	<p>AU-5b [Assignment: Organization-defined actions to be taken] Parameter: [low-impact: overwrite oldest audit records; moderate-impact: shut down]</p>	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AU-6	Audit Review, Analysis, and Reporting	AU-6	AU-6 <b>AU-6 (1)</b> <b>AU-6 (3)</b>	AU-6a. [Assignment: organization-defined frequency] Parameter: [at least weekly]	None.
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 AU-7 (1)	None.	None.
AU-8	Time Stamps	AU-8	AU-8 AU-8 (1)	AU-8 (1) [Assignment: organization-defined frequency] Parameter: [at least hourly]  AU-8 (1) [Assignment: organization-defined authoritative time source] Parameter: [http://tf.nist.gov/tf-cgi/servers.cgi].	AU-8 (1)  Requirement: 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.  Requirement: 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.  Guidance: Synchronization of system clocks improves the accuracy of log analysis.
AU-9	Protection of Audit Information	AU-9	AU-9 <b>AU-9 (2)</b>	<b>AU-9 (2)</b> [Assignment: organization-defined frequency] Parameter: [at least weekly]	None.
AU-10	Non-Repudiation	Not Selected	<b>AU-10</b> <b>AU-10 (5)</b>	<b>AU-10 (5)</b> [Selection: FIPS-validated; NSA-approved] Parameter: See additional requirements and guidance.	<b>AU-10 (5)</b> Requirement: 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.
AU-11	Audit Record Retention	AU-11	AU-11	AU-11 [Assignment: organization-defined time period consistent with records retention policy] Parameter: [at least ninety days]	AU-11 Requirement: 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.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
AU-12	Audit Generation	AU-12	AU-12	AU-12a. [Assignment: organization-defined information system components] Parameter: [all information system components where audit capability is deployed]	None.
<b>1.4. Assessment and Authorization (CA)</b>					
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
CA-2	Security Assessments	CA-2 <b>CA-2 (1)</b>	CA-2 CA-2 (1)	CA-2b. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
CA-3	Information System Connections	CA-3	CA-3	None.	None.
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5b. [Assignment: organization-defined frequency] Parameter: [at least quarterly]	None.
CA-6	Security Authorization	CA-6	CA-6	CA-6c. [Assignment: organization-defined frequency] Parameter: [at least every three years or when a significant change occurs]	CA-6c. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would require a reauthorization of the information system. The types of changes are approved and accepted by the JAB.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CA-7	Continuous Monitoring	CA-7 <b>CA-7 (2)</b>	CA-7 <b>CA-7 (2)</b>	<p>CA-7d. [Assignment: organization-defined frequency] Parameter: [monthly]</p> <p><b>CA-7 (2)</b> [Assignment: organization-defined frequency] Parameter: [annually]</p> <p>[Selection: announced; unannounced] Parameter: [unannounced]</p> <p>[Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises] Parameter: [penetration testing]</p> <p>[Assignment: organization-defined other forms of security assessment] Parameter: [in-depth monitoring]</p>	None.
<b>1.5. Configuration Management (CM)</b>					
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	<p>CM-1 [Assignment: organization-defined frequency] Parameter: [at least annually]</p>	None.
CM-2	Baseline Configuration	CM-2	<p>CM-2 CM-2 (1) CM-2 (3) <b>CM-2 (5)</b></p>	<p>CM-2 (1) (a) [Assignment: organization-defined frequency] Parameter: [annually]</p> <p>CM-2 (1) (b) [Assignment: organization-defined circumstances] Parameter: [a significant change]</p> <p><b>CM-2 (5) (a)</b> [Assignment: organization-defined list of software programs authorized to execute on the information system] Parameter: See additional requirements and guidance.</p>	<p>CM-2 (1) (b) Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F. The service provider describes the types of changes to the information system or the environment of operations that would require a review and update of the baseline configuration. The types of changes are approved and accepted by the JAB.</p> <p><b>CM-2 (5) (a)</b> Requirement: The service provider defines and maintains a list of software programs authorized to execute on the information system. The list of authorized programs is approved and accepted by the JAB.</p>

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CM-3	Configuration Change Control	<b>CM-3</b>	CM-3 CM-3 (2)	<p>CM-3f. [Assignment: organization-defined configuration change control element] Parameter: See additional requirements and guidance.</p> <p>[Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]] Parameter: See additional requirements and guidance.</p>	<p>CM-3f. Requirement: The service provider defines the configuration change control element and the frequency or conditions under which it is convened. The change control element and frequency/conditions of use are approved and accepted by the JAB.</p> <p>Requirement: 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.</p>
CM-4	Security Impact Analysis	CM-4	CM-4	None.	None.
CM-5	Access Restrictions for Change	Not Selected	CM-5 <b>CM-5 (1)</b> <b>CM-5 (5)</b>	<p><b>CM-5 (5) (b)</b> [Assignment: organization-defined frequency] Parameter: [at least quarterly]</p>	None.
CM-6	Configuration Settings	CM-6	CM-6 <b>CM-6 (1)</b> CM-6 (3)	<p>CM-6a. [Assignment: organization-defined security configuration checklists] Parameter: [United States Government Configuration Baseline (USGCB)]</p>	<p>CM-6a. Requirement: The service provider uses the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. Configuration settings are approved and accepted by the JAB.</p> <p>CM-6a Requirement: The service provider ensures that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available).</p> <p>CM-6a. Guidance: Information on the USGCB checklists can be found at: <a href="http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc">http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc</a>.</p>

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CM-7	Least Functionality	CM-7	CM-7 CM-7 (1)	<p>CM-7 [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services] Parameter: [United States Government Configuration Baseline (USGCB)]</p> <p>CM-7 (1) [Assignment: organization-defined frequency] Parameter: [at least quarterly]</p>	<p>CM-7 Requirement: The service provider uses the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. The list of prohibited or restricted functions, ports, protocols, and/or services is approved and accepted by the JAB.</p> <p>CM-7 Guidance: Information on the USGCB checklists can be found at: <a href="http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc">http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc</a>.</p>
CM-8	Information System Component Inventory	CM-8	CM-8 CM-8 (1) <b>CM-8 (3)</b> CM-8 (5)	<p>CM-8d. [Assignment: organization-defined information deemed necessary to achieve effective property accountability] Parameter: See additional requirements and guidance.</p> <p><b>CM-8 (3) (a)</b> [Assignment: organization-defined frequency] Parameter: [Continuously, using automated mechanisms with a maximum five-minute delay in detection.]</p>	<p>CM-8d. Requirement: The service provider defines information deemed necessary to achieve effective property accountability. Property accountability information is approved and accepted by the JAB.</p> <p>Guidance: Information deemed necessary to achieve effective property accountability may include hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.</p>
CM-9	Configuration Management Plan		CM-9	None.	None.
<b>1.6. Contingency Planning (CP)</b>					
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	<p>CP-1 [Assignment: organization-defined frequency] Parameter: [at least annually]</p>	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CP-2	Contingency Plan	CP-2	CP-2 CP-2 (1) <b>CP-2 (2)</b>	<p>CP-2b. [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements] Parameter: See additional requirements and guidance.</p> <p>CP-2d. [Assignment: organization-defined frequency] Parameter: [at least annually]</p> <p>CP-2f. [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements] Parameter: See additional requirements and guidance.</p>	<p>CP-2b. Requirement: The service provider defines a list of key contingency personnel (identified by name and/or by role) and organizational elements. The contingency list includes designated FedRAMP personnel.</p> <p>CP-2f. Requirement: The service provider defines a list of key contingency personnel (identified by name and/or by role) and organizational elements. The contingency list includes designated FedRAMP personnel.</p>
CP-3	Contingency Training	CP-3	CP-3	<p>CP-3 [Assignment: organization-defined frequency] Parameter: [at least annually]</p>	None.
CP-4	Contingency Plan Testing and Exercises	CP-4	CP-4 CP-4 (1)	<p>CP-4a. [Assignment: organization-defined frequency] Parameter: [at least annually for moderate impact systems; at least every three years for low impact systems]</p> <p>[Assignment: organization-defined tests and/or exercises] Parameter: [functional exercises for moderate impact systems; classroom exercises/table top written tests for low impact systems]</p>	<p>CP-4a. Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the JAB.</p>
CP-6	Alternate Storage Site	Not Selected	CP-6 CP-6 (1) CP-6 (3)	None.	None.
CP-7	Alternate Processing Site	Not Selected	CP-7 CP-7 (1) CP-7 (2) CP-7 (3) CP-7 (5)	<p>CP-7a. [Assignment: organization-defined time period consistent with recovery time objectives] Parameter: See additional requirements and guidance.</p>	<p>CP-7a. Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis. The time period is approved and accepted by the JAB.</p>

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
CP-8	Telecommunications Services	Not Selected	CP-8 CP-8 (1) CP-8 (2)	CP-8 [Assignment: organization-defined time period] Parameter: See additional requirements and guidance.	CP-8 Requirement: The service provider defines a time period consistent with the business impact analysis. The time period is approved and accepted by the JAB.
CP-9	Information System Backup	CP-9	CP-9 CP-9 (1) <b>CP-9 (3)</b>	CP-9a. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [daily incremental; weekly full]  CP-9b. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [daily incremental; weekly full]  CP-9c. [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives] Parameter: [daily incremental; weekly full]  CP-9 (1) [Assignment: organization-defined frequency] Parameter: [at least annually]	CP-9a. Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.  CP-9b. Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB.  CP-9c. Requirement: The service provider maintains 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. The backup storage capability is approved and accepted by the JAB.
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 CP-10 (2) CP-10 (3)	CP-10 (3) [Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state] Parameter: See additional requirements and guidance.	CP-10 (3) Requirement: The service provider defines 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.
<b>1.7. Identification and Authentication (IA)</b>					
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
IA-2	Identification and Authentication (Organizational Users)	IA-2 IA-2 (1)	IA-2 IA-2 (1) IA-2 (2) IA-2 (3) IA-2 (8)	IA-2 (8) [Assignment: organization-defined replay-resistant authentication mechanisms] Parameter: See additional requirements and guidance.	IA-2 (8) Requirement: The service provider defines replay-resistant authentication mechanisms. The mechanisms are approved and accepted by the JAB.
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3 [Assignment: organization-defined list of specific and/or types of devices] Parameter: See additional requirements and guidance.	IA-3 Requirement: The service provider defines a list a specific devices and/or types of devices. The list of devices and/or device types is approved and accepted by the JAB.
IA-4	Identifier Management	IA-4	IA-4 <b>IA-4 (4)</b>	IA-4d. [Assignment: organization-defined time period] Parameter: [at least two years]  IA-4e. [Assignment: organization-defined time period of inactivity] Parameter: [ninety days for user identifiers] Parameter: See additional requirements and guidance.  <b>IA-4 (4)</b> [Assignment: organization-defined characteristic identifying user status] Parameter: [contractors; foreign nationals]	IA-4e. Requirement: The service provider defines time period of inactivity for device identifiers. The time period is approved and accepted by JAB.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
IA-5	Authenticator Management	IA-5 IA-5 (1)	IA-5 IA-5 (1) IA-5 (2) IA-5 (3) <b>IA-5 (6)</b> <b>IA-5 (7)</b>	<p>IA-5g. [Assignment: organization-defined time period by authenticator type] Parameter: [sixty days]</p> <p>IA-5 (1) (a) [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type] Parameter: [case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters]</p> <p>IA-5 (1) (b) [Assignment: organization-defined number of changed characters] Parameter: [at least one or as determined by the information system (where possible)]</p> <p>IA-5 (1) (d) [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum] Parameter: [one day minimum, sixty day maximum]</p> <p>IA-5 (1) (e) [Assignment: organization-defined number] Parameter: [twenty four]</p> <p>IA-5 (3) [Assignment: organization-defined types of and/or specific authenticators] Parameter: [HSPD12 smart cards]</p>	IA-5 (1) (a) Guidance: Mobile devices are excluded from the password complexity requirement.
IA-6	Authenticator Feedback	IA-6	IA-6	None.	None.
IA-7	Cryptographic Module Authentication	IA-7	IA-7	None.	None.
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8	IA-8	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
<b>1.8. Incident Response (IR)</b>					
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
IR-2	Incident Response Training	IR-2	IR-2	IR-2b. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 [Assignment: organization-defined frequency] Parameter: [annually]  [Assignment: organization-defined tests and/or exercises] Parameter: See additional requirements and guidance.	IR-3 Requirement: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended).  IR-3 Requirement: The service provider provides test plans to FedRAMP annually. Test plans are approved and accepted by the JAB prior to test commencing.
IR-4	Incident Handling	IR-4	IR-4 IR-4 (1)	None.	IR-4 Requirement: 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.
IR-5	Incident Monitoring	IR-5	IR-5	None.	None.
IR-6	Incident Reporting	IR-6	IR-6 IR-6 (1)	IR-6a. [Assignment: organization-defined time period] Parameter: [US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended)]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
IR-7	Incident Response Assistance	IR-7	IR-7 IR-7 (1) <b>IR-7 (2)</b>	None.	None.
IR-8	Incident Response Plan	IR-8	IR-8	IR-8b. <i>[Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements]</i> Parameter: See additional requirements and guidance.  IR-8c. <i>[Assignment: organization-defined frequency]</i> Parameter: [at least annually]  IR-8e. <i>[Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements]</i> Parameter: See additional requirements and guidance.	IR-8b. Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.  IR-8e. Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.
<b>1.9. Maintenance (MA)</b>					
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1 <i>[Assignment: organization-defined frequency]</i> Parameter: [at least annually]	None.
MA-2	Controlled Maintenance	MA-2	MA-2 MA-2 (1)	None.	None.
MA-3	Maintenance Tools	Not Selected	MA-3 MA-3 (1) MA-3 (2) <b>MA-3 (3)</b>	None.	None.
MA-4	Non-Local Maintenance	MA-4	MA-4 MA-4 (1) MA-4 (2)	None.	None.
MA-5	Maintenance Personnel	MA-5	MA-5	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
MA-6	Timely Maintenance	Not Selected	MA-6	<p>MA-6                      [Assignment: organization-defined list of security-critical information system components and/or key information technology components]                      Parameter: See additional requirements and guidance.</p> <p>[Assignment: organization-defined time period]                      Parameter: See additional requirements and guidance.</p>	<p>MA-6                      Requirement: The service provider defines a list of security-critical information system components and/or key information technology components. The list of components is approved and accepted by the JAB.</p> <p>Requirement: The service provider defines a time period to obtain maintenance and spare parts in accordance with the contingency plan for the information system and business impact analysis. The time period is approved and accepted by the JAB.</p>
<b>1.10. Media Protection (MP)</b>					
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	<p>MP-1                      [Assignment: organization-defined frequency]                      Parameter: [at least annually]</p>	None.
MP-2	Media Access	MP-2	MP-2 MP-2 (1)	<p>MP-2                      [Assignment: organization-defined types of digital and non-digital media]                      Parameter: See additional requirements and guidance.</p> <p>[Assignment: organization-defined list of authorized individuals]                      Parameter: See additional requirements and guidance.</p> <p>[Assignment: organization-defined security measures]                      Parameter: See additional requirements and guidance.</p>	<p>MP-2                      Requirement: The service provider defines types of digital and non-digital media. The media types are approved and accepted by the JAB.</p> <p>Requirement: The service provider defines a list of individuals with authorized access to defined media types. The list of authorized individuals is approved and accepted by the JAB.</p> <p>Requirement: The service provider defines the types of security measures to be used in protecting defined media types. The security measures are approved and accepted by the JAB.</p>
MP-3	Media Marking	Not Selected	MP-3	<p>MP-3b.                      [Assignment: organization-defined list of removable media types]                      Parameter: [no removable media types]</p> <p>[Assignment: organization-defined controlled areas]                      Parameter: [not applicable]</p>	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
MP-4	Media Storage	Not Selected	MP-4 MP-4 (1)	MP-4a. <i>[Assignment: organization-defined types of digital and non-digital media]</i> Parameter: [magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks]  <i>[Assignment: organization-defined controlled areas]</i> Parameter: See additional requirements and guidance.  <i>[Assignment: organization-defined security measures]</i> Parameter: [for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secure storage in locked cabinets or safes]	MP-4a. Requirement: The service provider defines controlled areas within facilities where the information and information system reside.
MP-5	Media Transport	Not Selected	MP-5 MP-5 (2) MP-5 (4)	MP-5a. <i>[Assignment: organization-defined types of digital and non-digital media]</i> Parameter: [magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks]  <i>[Assignment: organization-defined security measures]</i> Parameter: [for digital media, encryption using a FIPS 140-2 validated encryption module]	MP-5a. Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB.
MP-6	Media Sanitization	MP-6	MP-6 <b>MP-6 (4)</b>	None.	None.
<b>1.11. Physical and Environmental Protection (PE)</b>					
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1 <i>[Assignment: organization-defined frequency]</i> Parameter: [at least annually]	None.
PE-2	Physical Access Authorizations	PE-2	PE-2 <b>PE-2 (1)</b>	PE-2c. <i>[Assignment: organization-defined frequency]</i> Parameter: [at least annually]	<b>PE-2 (1)</b> Requirement: The service provider provides physical access to the facility where information systems reside based on position, role, and need-to-know.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
PE-3	Physical Access Control	PE-3	PE-3	PE-3f. [Assignment: organization-defined frequency] Parameter: [at least annually]  PE-3g. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
PE-4	Access Control for Transmission Medium	Not Selected	PE-4	None.	None.
PE-5	Access Control for Output Devices	Not Selected	PE-5	None.	None.
PE-6	Monitoring Physical Access	PE-6	PE-6 PE-6 (1)	PE-6b. [Assignment: organization-defined frequency] Parameter: [at least semi-annually]	None.
PE-7	Visitor Control	PE-7	PE-7 PE-7 (1)	None.	None.
PE-8	Access Records	PE-8	PE-8	PE-8b. [Assignment: organization-defined frequency] Parameter: [at least monthly]	None.
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	None.	None.
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10b. [Assignment: organization-defined location by information system or system component] Parameter: See additional requirements and guidance.	PE-10b. Requirement: The service provider defines emergency shutoff switch locations. The locations are approved and accepted by the JAB.
PE-11	Emergency Power	Not Selected	PE-11 <b>PE-11 (1)</b>	None.	None.
PE-12	Emergency Lighting	PE-12	PE-12	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
PE-13	Fire Protection	PE-13	PE-13 PE-13 (1) PE-13 (2) PE-13 (3)	None.	None.
PE-14	Temperature and Humidity Controls	PE-14	PE-14 <b>PE-14 (1)</b>	PE-14a. [Assignment: organization-defined acceptable levels] Parameter: [consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled <i>Thermal Guidelines for Data Processing Environments</i> ]  PE-14b. [Assignment: organization-defined frequency] Parameter: [continuously]	PE-14a. Requirements: The service provider measures temperature at server inlets and humidity levels by dew point.
PE-15	Water Damage Protection	PE-15	PE-15	None.	None.
PE-16	Delivery and Removal	PE-16	PE-16	PE-16 [Assignment: organization-defined types of information system components] Parameter: [all information system components]	None.
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17a. [Assignment: organization-defined management, operational, and technical information system security controls] Parameter: See additional requirements and guidance.	PE-17a. Requirement: The service provider defines management, operational, and technical information system security controls for alternate work sites. The security controls are approved and accepted by the JAB.
PE-18	Location of Information System Components	Not Selected	PE-18	None.	None.
<b>1.12. Planning (PL)</b>					
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
PL-2	System Security Plan	PL-2	PL-2 <b>PL-2 (2)</b>	PL-2b. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
PL-4	Rules of Behavior	PL-4	PL-4	None.	None.
PL-5	Privacy Impact Assessment	PL-5	PL-5	None.	None.
PL-6	Security-Related Activity Planning	<b>PL-6</b>	PL-6	None.	None.
<b>1.13. Personnel Security (PS)</b>					
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
PS-2	Position Categorization	PS-2	PS-2	PS-2c. [Assignment: organization-defined frequency] Parameter: [at least every three years]	None.
PS-3	Personnel Screening	PS-3	PS-3	PS-3b. [Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening] Parameter: [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]	None.
PS-4	Personnel Termination	PS-4	PS-4	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
PS-5	Personnel Transfer	PS-5	PS-5	PS-5 [Assignment: organization-defined transfer or reassignment actions] Parameter: See additional requirements and guidance.  [Assignment: organization-defined time period following the formal transfer action] Parameter: [within five days]	PS-5 Requirement: The service provider defines transfer or reassignment actions. Transfer or reassignment actions are approved and accepted by the JAB.
PS-6	Access Agreements	PS-6	PS-6	PS-6b. [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
PS-7	Third-Party Personnel Security	PS-7	PS-7	None.	None.
PS-8	Personnel Sanctions	PS-8	PS-8	None.	None.
<b>1.14. Risk Assessment (RA)</b>					
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
RA-2	Security Categorization	RA-2	RA-2	None.	None.
RA-3	Risk Assessment	RA-3	RA-3	RA-3b. [Selection: security plan; risk assessment report; [Assignment: organization-defined document]] Parameter: [security assessment report]  RA-3c. [Assignment: organization-defined frequency] Parameter: [at least every three years or when a significant change occurs]  RA-3d. [Assignment: organization-defined frequency] Parameter: [at least every three years or when a significant change occurs]	RA-3c. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.  RA-3d. Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
RA-5	Vulnerability Scanning	RA-5 <b>RA-5 (1)</b> <b>RA-5 (2)</b> <b>RA-5 (3)</b> <b>RA-5 (9)</b>	RA-5 RA-5 (1) <b>RA-5 (2)</b> <b>RA-5 (3)</b> <b>RA-5 (9)</b> <b>RA-5 (6)</b>	RA-5a. [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] Parameter: [quarterly operating system, web application, and database scans (as applicable)]  RA-5d. Assignment: organization-defined response times Parameter: [high-risk vulnerabilities mitigated within thirty days; moderate risk vulnerabilities mitigated within ninety days]  <b>RA-5 (2)</b> [Assignment: organization-defined frequency] Parameter: [continuously, before each scan]	None.
<b>1.15. System and Services Acquisition (SA)</b>					
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
SA-2	Allocation of Resources	SA-2	SA-2	None.	None.
SA-3	Life Cycle Support	SA-3	SA-3	None.	None.
SA-4	Acquisitions	SA-4	SA-4 SA-4 (1) SA-4 (4) <b>SA-4 (7)</b>	None.	SA-4 Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred. See <a href="http://www.niap-ccevs.org/vpl">http://www.niap-ccevs.org/vpl</a> or <a href="http://www.commoncriteriaportal.org/products.html">http://www.commoncriteriaportal.org/products.html</a> .
SA-5	Information System Documentation	SA-5	SA-5 SA-5 (1) SA-5 (3)	None.	None.
SA-6	Software Usage Restrictions	SA-6	SA-6	None.	None.
SA-7	User-Installed Software	SA-7	SA-7	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SA-8	Security Engineering Principles	Not Selected	SA-8	None.	None.
SA-9	External Information System Services	SA-9	SA-9 <b>SA-9 (1)</b>	<b>SA-9 (1) (b)</b> [Assignment: organization-defined senior organizational official]. Parameter: [Joint Authorization Board (JAB)]	<b>SA-9 (1)</b> Requirement: 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.
SA-10	Developer Configuration Management	Not Selected	SA-10	None.	None.
SA-11	Developer Security Testing	<b>SA-11</b> <b>SA-11 (1)</b>	SA-11 <b>SA-11 (1)</b>	None.	<b>SA-11 (1)</b> Requirement: The service provider submits a code analysis report as part of the authorization package and updates the report in any reauthorization actions.  <b>SA-11 (1)</b> Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.
SA-12	Supply Chain Protection	Not Selected	<b>SA-12</b>	SA-12 [Assignment: organization-defined list of measures to protect against supply chain threats] Parameter: See additional requirements and guidance.	SA-12 Requirement: The service provider defines a list of measures to protect against supply chain threats. The list of protective measures is approved and accepted by JAB.
<b>1.16. System and Communications Protection (SC)</b>					
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SC-2	Application Partitioning	Not Selected	SC-2	None.	None.
SC-4	Information in Shared Resources	Not Selected	SC-4	None.	None.
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5 [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list] Parameter: See additional requirements and guidance.	SC-5 Requirement: The service provider defines a list of types of denial of service attacks (including but not limited to flooding attacks and software/logic attacks) or provides a reference to source for current list. The list of denial of service attack types is approved and accepted by JAB.
SC-6	Resource Priority	Not Selected	<b>SC-6</b>	None	None.
SC-7	Boundary Protection	SC-7	SC-7 SC-7 (1) SC-7 (2) SC-7 (3) SC-7 (4) SC-7 (5) SC-7 (7) <b>SC-7 (8)</b> <b>SC-7 (12)</b> <b>SC-7 (13)</b> <b>SC-7 (18)</b>	SC-7 (4) (e) [Assignment: organization-defined frequency] Parameter: [at least annually] <b>SC-7 (8)</b> [Assignment: organization-defined internal communications traffic] Parameter: See additional requirements and guidance. [Assignment: organization-defined external networks] Parameter: See additional requirements and guidance. <b>SC-7 (13)</b> [Assignment: organization-defined key information security tools, mechanisms, and support components] Parameter: See additional requirements and guidance.	SC-7 (1) Requirement: 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.  <b>SC-7 (8)</b> Requirements: The service provider defines the internal communications traffic to be routed by the information system through authenticated proxy servers and the external networks that are the prospective destination of such traffic routing. The internal communications traffic and external networks are approved and accepted by JAB.  <b>SC-7 (13)</b> Requirement: The service provider defines 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 or logically separate subnets.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SC-8	Transmission Integrity	Not Selected	SC-8 SC-8 (1)	None.	None.
SC-9	Transmission Confidentiality	Not Selected	SC-9 SC-9 (1)	SC-9 (1) [Assignment: <i>organization-defined alternative physical measures</i> ] Parameter: See additional requirements and guidance	SC-9(1) Requirement: The service provider must implement a hardened or alarmed carrier Protective Distribution System (PDS) when transmission confidentiality cannot be achieved through cryptographic mechanisms.
SC-10	Network Disconnect	Not Selected	SC-10	SC-10 [Assignment: <i>organization-defined time period</i> ] Parameter: [thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users]	SC-10 Guidance: Long running batch jobs and other operations are not subject to this time limit.
SC-11	Trusted Path	Not Selected	<b>SC-11</b>	<b>SC-11</b> [Assignment: <i>organization-defined security functions to include at a minimum, information system authentication and re-authentication</i> ] Parameter: See additional requirements and guidance	<b>SC-11</b> Requirement: The service provider defines the 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). The list of security functions requiring a trusted path is approved and accepted by JAB.
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12 <b>SC-12 (2)</b> <b>SC-12 (5)</b>	SC-12 (2) [Selection: <i>NIST-approved, NSA-approved</i> ] Parameter: [NIST-approved]	None.
SC-13	Use of Cryptography	SC-13	SC-13 <b>SC-13 (1)</b>	None.	None.
SC-14	Public Access Protections	SC-14	SC-14	None.	None.
SC-15	Collaborative Computing Devices	SC-15	SC-15	SC-15a. [Assignment: <i>organization-defined exceptions where remote activation is to be allowed</i> ] Parameter: [no exceptions]	SC-15 Requirement: The information system provides <i>disablement</i> (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SC-16	Transmission of Security Attributes	Not Selected	<b>SC-16</b>	None.	None.
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17 [Assignment: organization-defined certificate policy] Parameter: See additional requirements and guidance.	SC-17 Requirement: The service provider defines the public key infrastructure certificate policy. The certificate policy is approved and accepted by the JAB.
SC-18	Mobile Code	<b>SC-18</b>	SC-18 <b>SC-18 (4)</b>	SC-18 (4) [Assignment: organization-defined software applications] Parameter: See additional requirements and guidance.  [Assignment: organization-defined actions] Parameter: See additional requirements and guidance.	SC-18 (4) Requirement: The service provider defines the software applications where the automatic execution of mobile code is prevented by the information system providing cloud services.  Requirement: The service provider defines the actions to be taken prior to the information system executing mobile code in the software applications identified. Software applications and actions taken by the service provider are approved by JAB.
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	None.	None.
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20 SC-20 (1)	SC-20 SC-20 (1)	None.	None.
SC-21	Secure Name/ Address Resolution Service (Recursive or Caching Resolver)	Not Selected	<b>SC-21</b>	None.	None.
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	None.	None.
SC-23	Session Authenticity	Not Selected	SC-23	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SC-25	Thin Nodes	Not Selected	<b>SC-25</b>	None	None.
SC-27	Operating System-Independent Applications	Not Selected	<b>SC-27</b>	<b>SC-27</b> [Assignment: organization-defined operating system independent applications]. Parameter: See additional requirements and guidance	<b>SC-27</b> Requirement: The service provider and service consumer define which applications must run independent of operating system. The OS Independent applications list is approved and accepted by JAB.
SC-28	Protection of Information at Rest	Not Selected	SC-28 <b>SC-28 (1)</b>	None.	None.
SC-30	Virtualization Techniques	Not Selected	<b>SC-30</b>	None	None.
SC-32	Information System Partitioning	Not Selected	SC-32	None.	None.
SC-33	Transmission Preparation Integrity	Not Selected	<b>SC-33</b>	None.	None.
<b>1.17. System and Information Integrity (SI)</b>					
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1 [Assignment: organization-defined frequency] Parameter: [at least annually]	None.
SI-2	Flaw Remediation	SI-2	SI-2 SI-2 (2)	SI-2 (2) [Assignment: organization-defined frequency] Parameter: [at least monthly]	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SI-3	Malicious Code Protection	SI-3	SI-3 SI-3 (1) SI-3 (2) SI-3 (3)	SI-3c. [Assignment: organization-defined frequency] Parameter: [at least weekly]  [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] Parameter: [block or quarantine malicious code, send alert to administrator, send alert to FedRAMP}	None.
SI-4	Information System Monitoring	<b>SI-4</b>	SI-4 SI-4 (2) SI-4 (4) SI-4 (5) SI-4 (6)	SI-4a. [Assignment: organization-defined monitoring objectives] Parameter: [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]  SI-4 (5) [Assignment: organization-defined list of compromise indicators] Parameter: [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]	SI-4(5) Requirement: The service provider defines additional compromise indicators as needed.  Guidance: Alerts may be generated from a variety of sources including but not limited to malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SI-5	Security Alerts, Advisories, and Directives	SI-5	SI-5	SI-5c. [Assignment: organization-defined list of personnel (identified by name and/or by role)] Parameter: [All staff with system administration, monitoring, and/or security responsibilities including but not limited to FedRAMP]	SI-5c. Requirement: The service provider defines a list of personnel (identified by name and/or by role) with system administration, monitoring, and/or security responsibilities who are to receive security alerts, advisories, and directives. The list also includes designated FedRAMP personnel.
SI-6	Security functionality verification	Not Selected	<b>SI-6</b>	<b>SI-6</b> [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] Parameter: [upon system startup and/or restart and periodically every ninety days]  [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] Parameter: [notifies system administrator]	None.
SI-7	Software and Information Integrity	Not Selected	SI-7 SI-7 (1)	SI-7 (1) [Assignment: organization-defined frequency] Parameter: [at least monthly]	None.
SI-8	Spam Protection	Not Selected	SI-8	None.	None.
SI-9	Information Input Restrictions	Not Selected	SI-9	None.	None.
SI-10	Information Input Validation	<b>SI-10</b>	SI-10	None.	None.

Control Number and Name		Control Baseline		Control Parameter Requirements	Additional Requirements and Guidance
		Low	Moderate		
SI-11	Error Handling	Not Selected	SI-11	SI-11b. [Assignment: organization-defined sensitive or potentially harmful information] Parameter: [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)].	None.
SI-12	Information Output Handling and Retention	SI-12	SI-12	None.	None.

123 **Table 1: FedRAMP Security Controls & Enhancements.**

# Chapter Two: Continuous Monitoring

## 124 2. Continuous Monitoring

### 125 2.1. Introduction

126 A critical aspect of managing risk to information from the operation and use of information  
127 systems involves the continuous monitoring of the security controls employed within or inherited  
128 by the system. Conducting a thorough point-in-time assessment of the deployed security controls  
129 is a necessary but not sufficient condition to demonstrate security due diligence. An effective  
130 organizational information security program also includes a rigorous continuous monitoring  
131 program integrated into the System Development Life Cycle (SDLC). The objective of the  
132 continuous monitoring program is to determine if the set of deployed security controls continue  
133 to be effective over time in light of the inevitable changes that occur. Continuous monitoring is a  
134 proven technique to address the security impacts on an information system resulting from  
135 changes to the hardware, software, firmware, or operational environment. A well-designed and  
136 well-managed continuous monitoring program can effectively transform an otherwise static  
137 security control assessment and risk determination process into a dynamic process that provides  
138 essential, near real-time security status-related information to organizational officials in order to  
139 take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding  
140 the operation of the information system. Continuous monitoring programs provide organizations  
141 with an effective mechanism to update *Security Plans*, *Security Assessment Reports*, and *Plans of*  
142 *Action and Milestones (POA&Ms)*.

143 An effective continuous monitoring program includes:

- 144 • Configuration management and control processes for information systems;
- 145 • Security impact analyses on proposed or actual changes to information systems and  
146 environments of operation;
- 147 • Assessment of selected security controls (including system-specific, hybrid, and common  
148 controls) based on the defined continuous monitoring strategy;
- 149 • Security status reporting to appropriate officials; and
- 150 • Active involvement by authorizing officials in the ongoing management of information  
151 system-related security risks.

### 152 2.2. Purpose

153 The purpose of this chapter is to establish and define how Continuous Monitoring will work in a  
154 cloud computing environment and specifically within the FedRAMP framework. This document  
155 will also serve to define reporting responsibilities and frequency for the Cloud Service Offering  
156 Service Provider (CSP).

### 157 2.3. Background

158 Service Provider is required to develop a strategy and implement a program for the continuous  
159 monitoring of security control effectiveness including the potential need to change or supplement  
160 the control set, taking into account any proposed/actual changes to the information system or its  
161 environment of operation. Continuous monitoring is integrated into the organization's system  
162 development life cycle processes. Robust continuous monitoring requires the active involvement  
163 of information system owners and common control providers, chief information officers, senior

164 information security officers, and authorizing officials. Continuous monitoring allows an  
165 organization to: (i) track the security state of an information system on a continuous basis; and  
166 (ii) maintain the security authorization for the system over time in highly dynamic environments  
167 of operation with changing threats, vulnerabilities, technologies, and missions/business  
168 processes. Continuous monitoring of security controls using automated support tools facilitates  
169 near real-time risk management and represents a significant change in the way security  
170 authorization activities have been employed in the past. Near real-time risk management of  
171 information systems can be accomplished by employing automated support tools to execute  
172 various steps in the Risk Management Framework including authorization-related activities. In  
173 addition to vulnerability scanning tools, system and network monitoring tools, and other  
174 automated support tools that can help to determine the security state of an information system,  
175 organizations can employ automated security management and reporting tools to update key  
176 documents in the authorization package including the security plan, security assessment report,  
177 and plan of action and milestones. The documents in the authorization package are considered  
178 “living documents” and updated accordingly based on actual events that may affect the security  
179 state of the information system.

## 180 2.4. Continuous Monitoring Requirements

181 FedRAMP is designed to facilitate a more streamlined approach and methodology to continuous  
182 monitoring. Accordingly, service providers must demonstrate their ability to perform routine  
183 tasks on a specifically defined scheduled basis to monitor the cyber security posture of the  
184 defined IT security boundary. While FedRAMP will not prescribe specific toolsets to perform  
185 these functions, FedRAMP does prescribe their minimum capabilities. Furthermore, FedRAMP  
186 will prescribe specific reporting criteria that service providers can utilize to maximize their  
187 FISMA reporting responsibilities while minimizing the resource strain that is often experienced.

## 188 2.5. Reporting and Continuous Monitoring

189 Maintenance of the security Authority To Operate (ATO) will be through continuous monitoring  
190 of security controls of the service providers system and its environment of operation to determine  
191 if the security controls in the information system continue to be effective over time in light of  
192 changes that occur in the system and environment. Through continuous monitoring, security  
193 controls and supporting deliverables are updated and submitted to FedRAMP per the schedules  
194 below. The submitted deliverables provide a current understanding of the security state and risk  
195 posture of the information systems. They allow FedRAMP authorizing officials to make credible  
196 risk-based decisions regarding the continued operations of the information systems and initiate  
197 appropriate responses as needed when changes occur. The deliverable frequencies below are to  
198 be considered standards. However, there will be instances, beyond the control of FedRAMP in  
199 which deliverables may be required on an ad hoc basis.

200 The deliverables required during continuous monitoring are depicted in Table 2: FedRAMP  
201 Continuous Monitoring . This table provides a listing of the deliverables, responsible party and  
202 frequency for completion. The table is organized into:

- 203 • **Deliverable** – Detailed description of the reporting artifact. If the artifact is expected in a  
204 specific format, that format appears in **BOLD** text.
- 205 • **Frequency** – Frequency under which the artifact should be created and/or updated.

206  
207

- **Responsibility** – Whether FedRAMP or the Cloud Service Provider is responsible for creation and maintenance of the artifact.

Deliverable	Frequency	Responsibility	
		FedRAMP	Cloud Service Provider
Scan reports of all systems within the boundary for vulnerability (Patch) management. <b>(Tool Output Report)</b>	Monthly		✓
Scan for verification of FDCC compliance (USGCB, CIS). <b>(SCAP Tool Output)</b>	Quarterly		✓
Incident Response Plan.	Annually		✓
POAM Remediation <b>(Completed POA&amp;M Matrix)</b>	Quarterly		✓
Change Control Process	Annually		✓
Penetration testing <b>(Formal plan and results)</b>	Annually	✓	✓
IV&V of controls	Semi-Annually	✓	
Scan to verify that boundary has not changed (also that no rogue systems are added after ATO) <b>(Tool Output Report)</b>	Quarterly		✓
System configuration management software <b>(SCAP Tool Output)</b>	Quarterly		✓
FISMA Reporting data	Quarterly		✓
Update Documentation	Annually		✓
Contingency Plan and Test Report	Annually		✓
Separation of Duties Matrix	Annually		✓
Information Security Awareness and Training Records Results)	Annually		✓

208 **Table 2: FedRAMP Continuous Monitoring Deliverables**

## 209 **2.6. Routine Systems Change Control Process**

210 The Change Control Process is instrumental in ensuring the integrity of the cloud computing  
211 environment. As the system owners as well as other authorizing officials approve changes, they  
212 are systematically documented. This documentation is a critical aspect of continuous monitoring  
213 since it establishes all of the requirements that led to the need for the change as well as the  
214 specific details of the implementation. To ensure that changes to the enterprise do not alter the  
215 security posture beyond the parameters set by the FedRAMP Joint Authorization Board (JAB),  
216 the key documents in the authorization package which include the security plan, security  
217 assessment report, and plan of action and milestones are updated and formally submitted to  
218 FedRAMP within 30 days of approved modification.

219 There are however, changes that are considered to be routine. These changes can be standard  
220 maintenance, addition or deletion of users, the application of standard security patches, or other  
221 routine activities. While these changes individually may not have much effect on the overall  
222 security posture of the system, in aggregate they can create a formidable security issue. To  
223 combat this possibility, these routine changes should be documented as part of the CSP's  
224 standard change management process and accounted for via the CSP's internal continuous  
225 monitoring plan. Accordingly, these changes must be documented, at a minimum, within the  
226 current SSP of the system within 30 days of implementation.

### 227 **Configuration Change Control Process (CCP)**

228 Throughout the System Development Life Cycle (SDLC) system owners must be cognizant of  
229 changes to the system. Since systems routinely experience changes over time to accommodate  
230 new requirements, new technologies or new risks, they must be routinely analyzed in respect to  
231 the security posture. Minor changes typically have little impact to the security posture of a  
232 system. These changes can be standard maintenance, adding or deleting users, applying standard  
233 security patches, or other routine activities. However, significant changes require an added level  
234 of attention and action. NIST defines significant change as "*A significant change is defined as a  
235 change that is likely to affect the security state of an information system.*" Changes such as  
236 installing a new operating system, port modification, new hardware platforms, or changes to the  
237 security controls should automatically trigger a re-authorization of the system via the FedRAMP  
238 process.

239 Minor changes must be captured and documented in the SSP of the system within 30 days of  
240 implementation. This requirement should be part of the CSP's documented internal continuous  
241 monitoring plan. Once the SSP is updated, it must be submitted to FedRAMP, and a record of  
242 the change must be maintained internally.

243 Major or significant changes may require re-authorization via the FedRAMP process. In order to  
244 facilitate a re-authorization, it is the responsibility of both the CSP and the sponsoring agency to  
245 notify FedRAMP of the need to make such a significant change. FedRAMP will assist and  
246 coordinate with all stakeholders the necessary steps to ensure that the change is adequately  
247 documented, tested and approved.

## 248 **2.7. FISMA Reporting Requirements**

249 FISMA established the IT security reporting requirements. OMB in conjunction with DHS  
250 enforces these reporting requirements. FISMA reporting responsibilities must be clearly defined.

251 FedRAMP will coordinate with CSP's and agencies to gather data associated with the cloud  
252 service offering. Only data related to the documented system security boundary of the cloud  
253 service offering will be collected by FedRAMP and reported to OMB at the appropriate time and  
254 frequency. Agencies will maintain their reporting responsibilities for their internal systems that  
255 correspond to the inter-connection between the agency and the cloud service offering.

## 256 **2.8. On-going Testing of Controls and Changes to Security Controls** 257 **Process**

258 System owners and administrators have long maintained the responsibility for patch and  
259 vulnerability management. However, it has been proven time and again that this responsibility  
260 often requires a heavy use of resources as well as a documented, repeatable process to be carried  
261 out consistently and adequately. This strain on resources and lack of processes has opened the  
262 door to many malicious entities through improper patching, significant lapse in time between  
263 patch availability and patch implementation, and other security oversights. Routine system  
264 scanning and reporting is a vital aspect of continuous monitoring and thus, maintaining a robust  
265 cyber security posture.

266 Vulnerability patching is critical. Proprietary operating system vendors (POSV) are constantly  
267 providing patches to mitigate vulnerabilities that are discovered. In fact, regularly scheduled  
268 monthly patches are published by many POSV to be applied to the appropriate operating system.  
269 It is also the case that POSV will, from time to time, publish security patches that should be  
270 applied on systems as soon as possible due to the serious nature of the vulnerability. Systems  
271 running in virtual environment are not exempted from patching. In fact, not only are the  
272 operating systems running in a virtual environment to be patched routinely, but often-times the  
273 virtualization software itself is exposed to vulnerabilities and thus must be patched either via a  
274 vendor based solution or other technical solution.

275 Open source operating systems require patch and vulnerability management as well. Due to the  
276 open nature of these operating systems there needs to be a reliable distribution point for system  
277 administrators to safely and securely obtain the required patches. These patches are available at  
278 the specific vendors' website.

279 Database platforms, web platforms and applications, and virtually all other software applications  
280 come with their own security issues. It is not only prudent, but also necessary to stay abreast of  
281 all of the vulnerabilities that are represented by the IT infrastructure and applications that are in  
282 use.

283 While vulnerability management is indeed a difficult and daunting task, there are proven tools  
284 available to assist the system owner and administrator in discovering the vulnerabilities in a  
285 timely fashion. These tools must be updated prior to being run. Updates are available at the  
286 corresponding vendors' website.

287 With these issues in mind FedRAMP will require CSP's to provide the following:

- 288 • Monthly vulnerability scans of all servers. Tools used to perform the scan must be  
289 provided as well as the version number reflecting the latest update. A formal report of  
290 all vulnerabilities discovered, mitigated or the mitigating strategy. This report should list  
291 the vulnerabilities by severity and name. Specificity is crucial to addressing the security  
292 posture of the system. All "High" level vulnerabilities must be mitigated within thirty

293 days (30) days of discovery. “Moderate” level vulnerabilities must be mitigated within  
294 ninety (90) days of discovery. It is accepted that, at certain times, the application of  
295 certain security patches can cause negative effects on systems. In these situations, it is  
296 understood that compensating controls (workarounds) must be used to minimize system  
297 performance degradation while serving to mitigate the vulnerability. These  
298 “Workarounds” must be submitted to FedRAMP & the Sponsoring agency for  
299 acceptance. All reporting must reflect these activities.

- 300 • Quarterly FDCC and/or system configuration compliance scans, with a Security Content  
301 Automation Protocol (SCAP) validated tool, across the entire boundary, which verifies  
302 that all servers maintain compliance with the mandated FDCC and/or approved system  
303 configuration security settings.
- 304 • Weekly scans for malicious code. Internal scans must be performed with the appropriate  
305 updated toolset. Monthly reporting is required to be submitted to FedRAMP, where  
306 activity is summarized.
- 307 • All software operating systems and applications are required to be scanned by an  
308 appropriate tool to perform a thorough code review to discover malicious code.  
309 Mandatory reporting to FedRAMP must include tool used, tool configuration settings,  
310 scanning parameters, application scanned (name and version) and the name of the third  
311 party performing the scan. Initial report should be included with the SSP as part of the  
312 initial authorization package.
- 313 • Performance of the annual Self Assessment in accordance with NIST guidelines. CSP  
314 must perform a self-assessment annually or whenever a significant change occurs. This  
315 is necessary if there is to be a continuous awareness of the risk and security posture of the  
316 system.
- 317 • Quarterly POA&M remediation reporting. CSP must provide to FedRAMP a detailed  
318 matrix of POA&M activities using the supplied FedRAMP POA&M Template. This  
319 should include milestones met or milestones missed, resources required and validation  
320 parameters.
- 321 • Active Incident Response capabilities allow for suspect systems to be isolated and  
322 inspected for any unapproved or otherwise malicious applications.
- 323 • Quarterly boundary-wide scans are required to be performed on the defined boundary IT  
324 system inventory to validate the proper HW and SW configurations as well as search and  
325 discover rogue systems attached to the infrastructure. A summary report, inclusive of a  
326 detailed network architecture drawing must be provided to FedRAMP.
- 327 • Change Control Process meetings to determine and validate the necessity for suggested  
328 changes to HW/SW within the enterprise must be coordinated with FedRAMP to ensure  
329 that the JAB is aware of the changes being made to the system.

## 330 2.9. Incident Response

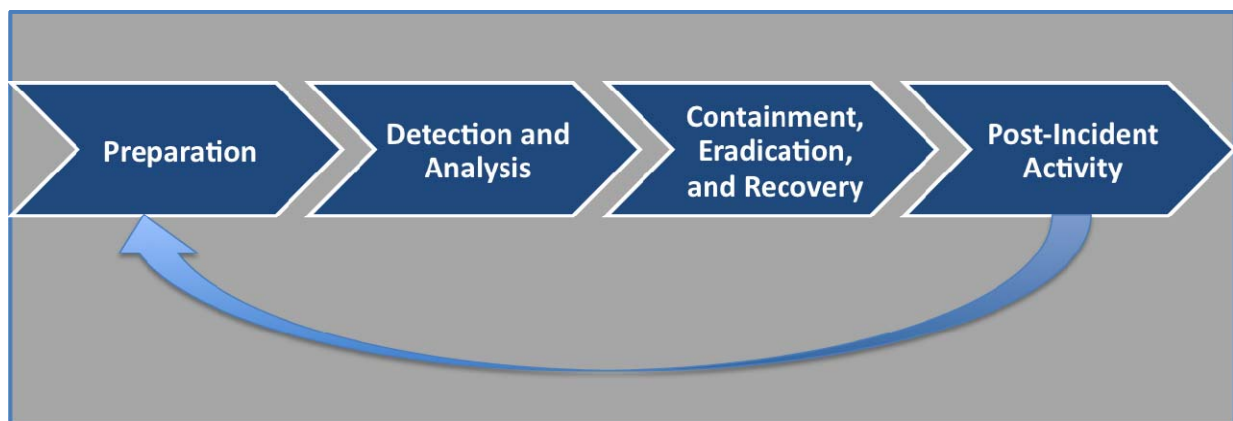
331 Computer security incident response has become an important component of information  
332 technology (IT) programs. Security-related threats have become not only more numerous and  
333 diverse but also more damaging and disruptive. New types of security-related incidents emerge  
334 frequently. Preventative activities based on the results of risk assessments can lower the number  
335 of incidents, but not all incidents can be prevented. An incident response capability is therefore  
336 necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the

337 weaknesses that were exploited, and restoring computing services. To that end, NIST SP 800-61  
338 provides guidelines for development and initiation of an incident handling program, particularly  
339 for analyzing incident-related data and determining the appropriate response to each incident.  
340 The guidelines can be followed independently of particular hardware platforms, operating  
341 systems, protocols, or applications. As part of the authorization process the system security plan  
342 will have documented all of the “IR” or Incident Response family of controls. One of these  
343 controls (IR-8) requires the development of an Incident Response plan that will cover the life  
344 cycle of incident response as documented in the NIST SP 800-61 guidelines. The plan should  
345 outline the resources and management support that is needed to effectively maintain and mature  
346 an incident response capability. The incident response plan should include these elements:

- 347 • Mission
- 348 • Strategies and goals
- 349 • Senior management approval
- 350 • Organizational approach to incident response
- 351 • How the incident response team will communicate with the rest of the organization
- 352 • Metrics for measuring the incident response capability
- 353 • Roadmap for maturing the incident response capability
- 354 • How the program fits into the overall organization.

355 The organization’s mission, strategies, and goals for incident response should help in  
356 determining the structure of its incident response capability. The incident response program  
357 structure should also be discussed within the plan. The response plan must address the  
358 possibility that incidents, including privacy breaches and classified spills, may impact the cloud  
359 and shared cloud customers. In any shared system, communication is the biggest key to success.

360 As part of the continuous monitoring of a system, responding to incidents will be a key element.  
361 The FedRAMP concern and its role in continuous monitoring will be to focus on how a provider  
362 conducted the incident response and any after incident actions. As represented in Figure 2:  
363 Incident response life cycle, incident response is a continually improving process.



364 **Figure 2: Incident response life cycle**  
365

366 One of the most important parts of incident response is also the most often omitted - learning and  
367 improving. Each incident response team should evolve to reflect new threats, improved

368 technology, and lessons learned. Many organizations have found that holding a “lessons learned”  
369 meeting with all involved parties after a major incident, and periodically after lesser incidents, is  
370 extremely helpful in improving security measures and the incident handling process itself. This  
371 meeting provides a chance to achieve closure with respect to an incident by reviewing what  
372 occurred, what was done to intervene, and how well intervention worked. The meeting should be  
373 held within several days of the end of the incident. Questions to be answered in the lessons  
374 learned meeting include:

- 375 • Exactly what happened, and at what times?
- 376 • How well did staff and management perform in dealing with the incident? Were the  
377 documented procedures followed? Were they adequate?
- 378 • What information was needed sooner?
- 379 • Were any steps or actions taken that might have inhibited the recovery?
- 380 • What would the staff and management do differently in a future occurrence?
- 381 • What corrective actions can prevent similar incidents in the future?
- 382 • What tools/resources are needed to detect, analyze, and mitigate future incidents?

383 Small incidents need limited post-incident analysis, with the exception of incidents performed  
384 through new attack methods that are of widespread concern and interest. After serious attacks  
385 have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and  
386 organizational boundaries to provide a mechanism for information sharing. The primary  
387 consideration in holding such meetings is ensuring that the right people are involved. Not only is  
388 it important to invite people who have been involved in the incident that is being analyzed, but  
389 also wise to consider who should be invited for the purpose of facilitating future cooperation.

## 390 **2.10. Independent Verification and Validation**

391 Independent Verification and Validation (IV&V) is going to be an integral component to a  
392 successful implementation of FedRAMP. With this in mind, it must be noted that establishing  
393 and maintaining an internal expertise of FedRAMP policies, procedures and processes is going to  
394 be required. This expertise will be tasked to perform various IV&V functions with CSP’s,  
395 sponsoring agencies and commercial entities obtained by CSP’s with absolute independence on  
396 behalf of FedRAMP. FedRAMP IV&V will be on behalf of the JAB.

397 As part of these efforts, FedRAMP will periodically perform audits (both scheduled and  
398 unscheduled) related strictly to the cloud computing service offering and the established system  
399 boundary. This will include, but not be limited to:

- 400 • Scheduled annual assessments of the system security documentation;
- 401 • Verification of testing procedures;
- 402 • Validation of testing tools and assessments;
- 403 • Validation of assessment methodologies employed by the CSP and independent  
404 assessors;
- 405 • Verification of the CSP continuous monitoring program; and
- 406 • Validation of CSP risk level determination criteria.

407 There are several methods that must be employed to accomplish these tasks. In accordance with  
408 the new FIMSA requirement, and as a matter of implementing industry best practices, FedRAMP  
409 IV&V will be performing penetration testing. This testing will be performed with strict

410 adherence to the specific guidelines established by a mutually agreed upon “Rules of  
411 Engagement” agreement between FedRAMP IV&V and the target stakeholders. *Unless*  
412 *otherwise stated in the agreement, all penetration testing will be passive in nature to avoid*  
413 *unintentional consequences.* No attempts to exploit vulnerabilities will be allowed unless  
414 specified within the “Rules of Engagement” agreement.

# Chapter Three: Potential Assessment & Authorization Approach

## 415 3. Potential Assessment & Authorization Approach

### 416 3.1. Introduction

417 Cloud computing presents a unique opportunity to increase the effectiveness and efficiency of  
418 the A&A and Continuous Monitoring process for Federal Agencies. The nature of cloud  
419 computing systems does not allow Federal Agencies to enforce their own unique security  
420 requirements and policies on a shared infrastructure – as many of these unique requirements are  
421 incompatible. Hence, cloud computing provides an opportunity for the Federal Agencies to work  
422 together to create a common security baseline for authorizing these shared systems.

423 The implementation of a common security baseline requires a joint approach for the A&A and  
424 Continuous Monitoring process. Any joint approach to this process requires a coordinated effort  
425 of many operational components working together. These operations need to interact/interplay  
426 with each other to successfully authorize and monitor cloud systems for government-wide use.

427 FedRAMP operations could potentially be executed by different entities and in many different  
428 models. However, the end goal is to establish an on-going A&A approach that all Federal  
429 Agencies can leverage. To accomplish that goal, the following benefits are desired regardless of  
430 the operating approach:

- 431 • Inter-Agency vetted Cloud Computing Security Requirement baseline that is used across  
432 the Federal Government;
- 433 • Consistent interpretation and application of security requirement baseline in a cloud  
434 computing environment;
- 435 • Consistent interpretation of cloud service provider authorization packages using a  
436 standard set of processes and evaluation criteria;
- 437 • More consistent and efficient continuous monitoring of cloud computing  
438 environment/systems fostering cross-agency communication in best practices and shared  
439 knowledge; and
- 440 • Cost savings/avoidance realized due to the “Approve once, use often” concept for  
441 security authorization of cloud systems.

442 FedRAMP operations could be conducted under many delivery models. The Federal Cloud  
443 Computing Initiative (FCCI) has focused on exploring three models in particular. The three  
444 models for assessment that have been vetted within Government and Industry are:

- 445 • A centralized approach working through a FedRAMP program office;
- 446 • A federated model using capabilities of multiple approved agency centers; and
- 447 • Some combination of the above that combines public and private sector partners.

448 Preliminary vetting of the three models focused on finding a model that best met the goals of this  
449 endeavor as mentioned above. As a result of vetting the models with government and industry  
450 stakeholders, this chapter presents FedRAMP operations through a centralized program office  
451 context. However, the government is seeking your input, knowledge, and experience as to the  
452 best model for FedRAMP operations that deliver upon the described benefits and encourage you  
453 to actively engage and contribute with substantive comments.

454

455 **3.2. Overview**

456 **Background**

457 The Federal Government is increasingly using large shared and outsourced systems by moving to  
458 cloud computing, virtualization, and datacenter/application consolidation. The current method of  
459 conducting risk management of shared, outsourced, cloud computing systems on an agency-by-  
460 agency basis causes duplication of efforts, inefficiencies in sharing knowledge, best practices and  
461 lessons learned in authorizing and ongoing monitoring of such systems, and the unnecessary cost  
462 from repetitive work and relearning.

463 In order to address these concerns, the U.S. Chief Information Officer (U.S. CIO) established a  
464 government-wide Federal Risk and Authorization Management Program (FedRAMP) to provide  
465 joint security assessment, authorizations and continuous monitoring of cloud computing services  
466 for all Federal Agencies to leverage.

467 **Purpose**

468 The objective of FedRAMP is threefold:

- 469 • Ensure that information systems/services used government-wide have adequate  
470 information security;
- 471 • Eliminate duplication of effort and reduce risk management costs; and
- 472 • Enable rapid and cost-effective procurement of information systems/services for Federal  
473 agencies.

474 **Benefits**

475 Joint authorization of cloud computing services provides a common security risk model that can  
476 be leveraged across the Federal Government. The use of a common security risk model provides  
477 a consistent baseline for Cloud based technologies across government. This common baseline  
478 will ensure that the benefits and challenges of cloud based technologies are effectively integrated  
479 across the various cloud computing solutions currently proposed within the government. The  
480 risk model will also enable the government to “approve once and use often” by ensuring other  
481 agencies gain the benefit and insight of the FedRAMP’s Authorization and access to service  
482 provider’s authorization packages.

483 By providing a unified government-wide risk management for enterprise level IT systems,  
484 FedRAMP will enable Agencies to either use or leverage authorizations with:

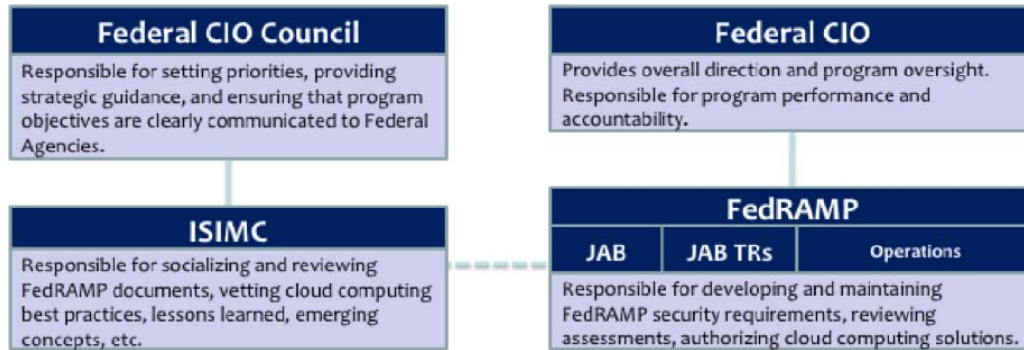
- 485 • An interagency vetted approach;
- 486 • Consistent application of Federal security requirements;
- 487 • Consolidated risk management; and
- 488 • Increased effectiveness and management cost savings.

489

490 **3.3. Governance**

491 The following sections describe the FedRAMP governance model and define the roles and  
 492 responsibilities of key stakeholders of the FedRAMP process.

493 **3.3.1. Governance Model**



494  
 495 **Figure 3: FedRAMP Governance Model**

496 FedRAMP is an interagency effort under the authority of the U.S. Chief Information Officer  
 497 (U.S. CIO) and managed out of the General Services Administration (GSA) as depicted in Figure  
 498 3 and detailed below.

499 The initiation of FedRAMP and the Joint Authorization Board (JAB) has been via the U.S. CIO  
 500 in coordination with the Federal CIO Council. The U.S. CIO has tasked the Joint Authorization  
 501 Board (JAB) with jointly authorizing cloud computing systems. The General Service  
 502 Administration has been tasked with the actual day-to-day operation of FedRAMP in supports  
 503 this effort.

504 The three permanent members of JAB include the Department of Homeland Security (DHS),  
 505 Department of Defense (DOD), and the General Services Administration (GSA). The sponsoring  
 506 government agency for each cloud computing system will be represented as the rotating JAB  
 507 member. The JAB also performs risk determination and acceptance of FedRAMP authorized  
 508 systems.

509 The JAB also has the final decision making authority on FedRAMP security controls, policies,  
 510 procedures and templates.

511 JAB technical representatives are appointed by their respective JAB authorizing official (both  
 512 permanent and rotating) for the implementation of the FedRAMP process. JAB technical  
 513 representatives provide subject matter expertise and advice to the JAB authorizing officials.

514 The JAB technical representatives review the vetted authorization packages provided by  
 515 FedRAMP. The JAB technical representatives make authorization recommendations to the JAB  
 516 authorizing officials and advise the JAB of all residual risks.

517 FedRAMP is an administrative support team provided by the U.S. CIO under the guidance of  
 518 GSA. FedRAMP operations are responsible for the day-to-day administration and project  
 519 management of FedRAMP. FedRAMP performs an initial review of submitted authorization  
 520 packages and has the authority to work with cloud computing system owners to refine each

521 submission until it satisfies FedRAMP and JAB requirements. FedRAMP also oversees  
 522 continuous monitoring of authorized systems.

523 The ISIMC under the Federal CIO Council is responsible for socializing and reviewing  
 524 FedRAMP processes and documents. They provide recommendations on the FedRAMP  
 525 documents directly to the JAB. Their recommendations are based on vetting the cloud computing  
 526 best practices, lessons learned and emerging concepts within the Federal CIO Council  
 527 community. However, the final approval on changes to FedRAMP processes and documents is  
 528 made by the JAB.

529 **3.3.2.Roles and Responsibilities**

530 Table 3: Stakeholder Roles and Responsibilities defines the responsibilities/tasks for FedRAMP  
 531 stakeholders.

Role	Duties and Responsibilities
<b>JAB Chair (U.S. CIO)</b>	<ul style="list-style-type: none"> <li>• Selects the JAB Authorizing Officials</li> <li>• Coordinates FedRAMP activities with the CIO Council</li> <li>• Tasks and funds FedRAMP, for technical support as necessary</li> </ul>
<b>JAB Authorizing Officials</b>	<ul style="list-style-type: none"> <li>• Designate a JAB Technical Representative</li> <li>• Ensure the Technical Representative considers current threats and evaluation criteria based on evolving cloud computing best practices in their review of joint authorizations.</li> <li>• Issue joint authorization decisions</li> <li>• Resolve issues as needed</li> </ul>
<b>JAB Rotating Authorizing Officials (Sponsoring Agency Authorizing Official)</b>	<ul style="list-style-type: none"> <li>• Same duties as JAB Authorizing Officials only for their sponsored cloud solution.</li> </ul>

Role	Duties and Responsibilities
<b>FedRAMP Operations</b>	<ul style="list-style-type: none"> <li>• Communicate FedRAMP security requirements to service providers or prospective providers.</li> <li>• Review CSP security authorization packages</li> <li>• Work with JAB Technical Representatives to clarify questions and concerns regarding authorization packages</li> <li>• Maintain a repository of Authorizations in two categories:                             <ul style="list-style-type: none"> <li>○ Authorizations granted by the JAB.</li> <li>○ Authorizations granted by individual agencies.</li> </ul> </li> <li>• Perform continuous monitoring oversight of FedRAMP authorized systems.</li> <li>• Collect FISMA data from FedRAMP authorized systems for quarterly and annually reporting of data to OMB through GSA.</li> <li>• Facilitate the leveraging of authorized systems for other federal entities.</li> <li>• Maintain knowledge of the FedRAMP capabilities and process throughout industry and the federal government.</li> </ul>
<b>JAB Technical Representatives (including the technical representative from the sponsoring Agency)</b>	<ul style="list-style-type: none"> <li>• Provide subject matter expertise to implement the direction of the JAB Authorizing Official.</li> <li>• Support FedRAMP in defining and implementing the joint authorization process.</li> <li>• Recommend authorization decisions to the JAB Authorizing Official.</li> <li>• Escalate issues to the JAB Authorizing Official as appropriate.</li> </ul>
<b>Sponsoring Agency</b>	<ul style="list-style-type: none"> <li>• Cloud system selection and submission to FedRAMP</li> <li>• Ensures a contractual agreement with a provider is in place using FedRAMP requirements.</li> <li>• Designate Federal personnel to facilitate the receipt and delivery of deliverables between the cloud computing provider (CSP) and FedRAMP.</li> <li>• Assessment, Authorization and continuous monitoring and FISMA reporting of controls that are Agency's (customer's) responsibility.</li> </ul>
<b>Leveraging Agency</b>	<ul style="list-style-type: none"> <li>• Review FedRAMP authorization packages.</li> <li>• Determine if the stated risk determination and acceptance is consistent with its agency's needs.</li> <li>• Authorize cloud system for their Agency use.</li> <li>• Assessment, Authorization and continuous monitoring and FISMA reporting of controls that are Agency's (customer's) responsibility.</li> </ul>

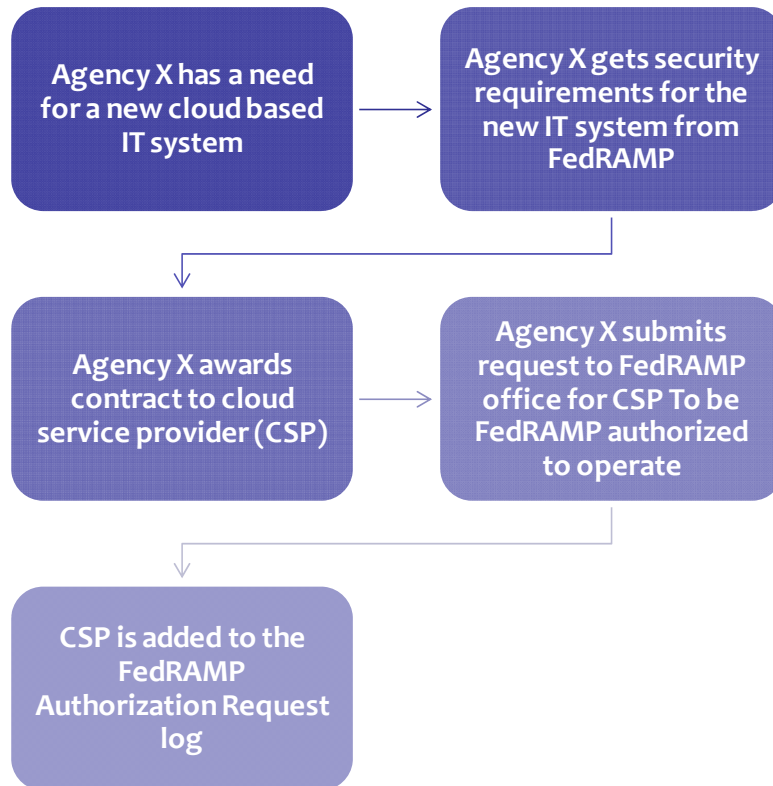
Role	Duties and Responsibilities
<p><b>Cloud Service Provider (CSP)</b></p>	<ul style="list-style-type: none"> <li>• The service provider is a government or commercial entity that has a cloud offering/service (IaaS, PaaS or SaaS) and requires FedRAMP authorization of their offering/service for Government use.</li> <li>• Work with the sponsoring Agency to submit their offering for FedRAMP authorization.</li> <li>• Hire independent third party assessor to perform initial system assessment and on-going monitoring of controls.</li> <li>• Create and submit authorization packages.</li> <li>• Provide Continuous Monitoring reports and updates to FedRAMP.</li> </ul>

532 **Table 3: Stakeholder Roles and Responsibilities**

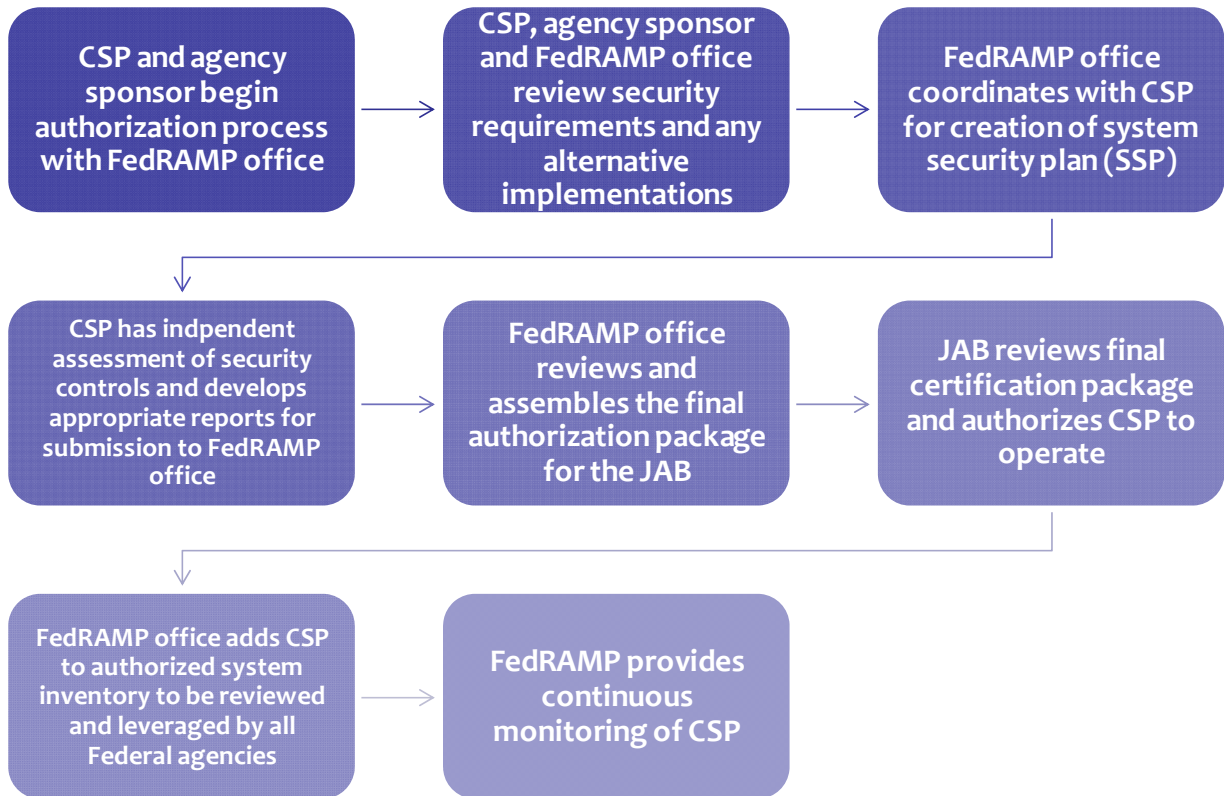
533 **3.4. Assessment and Authorization Processes**

534 **3.4.1.High-Level Overview**

535 The following figure depicts the high-level process for getting on the FedRAMP authorization  
536 request log. Once the Cloud Service Provider (CSP) system is officially on the FedRAMP  
537 authorization log, FedRAMP begins processing the cloud system for JAB authorization. The  
538 subsequent sections detail the steps involved in the FedRAMP Assessment and Authorization  
539 process.



540 **Figure 4: FedRAMP authorization request process**  
541



542  
543

Figure 5: FedRAMP authorization process

## 544 3.4.2. Detailed Assessment & Authorization Process

### 545 3.4.2.1. Purpose

546 This section defines FedRAMP assessment and authorization process for Cloud Service  
547 Providers (CSP). It also provides guidelines and procedures for applying the NIST 800-37 R1  
548 Risk Management Framework to include conducting the activities of security categorization,  
549 security control selection and implementation, security control assessment, information system  
550 authorization, and continuous monitoring. CCS Service Providers should use this process and  
551 the noted references prior to initiating/performing the Security Authorization process.

### 552 3.4.2.2. Policy

553 Security Authorization Process:

- 554 a. The FedRAMP Authorizing Officials (AO) must authorize, in writing, all cloud computing  
555 systems before they go into operational service for government interest.
- 556 b. A service provider's cloud computing systems must be authorized/reauthorized at least every  
557 three (3) years or whenever there is a significant change to the system's security posture in  
558 accordance with NIST SP 800-37 R1.

559 Authorization termination dates are influenced by FedRAMP policies that may establish  
560 maximum authorization periods. For example, if the maximum authorization period for an  
561 information system is three years, then the service provider establishes a continuous monitoring  
562 strategy for assessing a subset of the security controls employed within and inherited by the  
563 system during the authorization period. This strategy allows all security controls designated in  
564 the respective security plans to be assessed at least one time by the end of the three-year period.  
565 This also includes any common controls deployed external to service provider cloud computing  
566 systems. If the security control assessments are conducted by qualified assessors with the  
567 required degree of *independence* based on policies, appropriate security standards and  
568 guidelines, and the needs of the FedRAMP authorizing officials, the assessment results can be  
569 cumulatively applied to the reauthorization, thus supporting the concept of ongoing  
570 authorization. FedRAMP policies regarding ongoing authorization and formal reauthorization,  
571 if/when required, are consistent with federal directives, regulations, and/or policies.

### 572 3.4.2.3. Required Artifacts

573 All Service Providers' CCS must complete *and deliver the following artifacts* as part of the  
574 authorization process. Templates for these artifacts can be found in FedRAMP templates as  
575 described in reference materials:

- 576 • Privacy Impact Assessment (PIA)
- 577 • FedRAMP Test Procedures and Results
- 578 • Security Assessment Report (SAR)
- 579 • System Security Plan (SSP)
- 580 • IT System Contingency Plan (CP)
- 581 • IT System Contingency Plan (CP) Test Results
- 582 • Plan of Action and Milestones (POA&M)

- 583 • Continuous Monitoring Plan (CMP)
- 584 • FedRAMP Control Tailoring Workbook
- 585 • Control Implementation Summary Table
- 586 • Results of Penetration Testing
- 587 • Software Code Review
- 588 • Interconnection Agreements/Service Level Agreements/Memorandum of Agreements

### 589 3.4.2.4. Assessment and Authorization Process Workflow

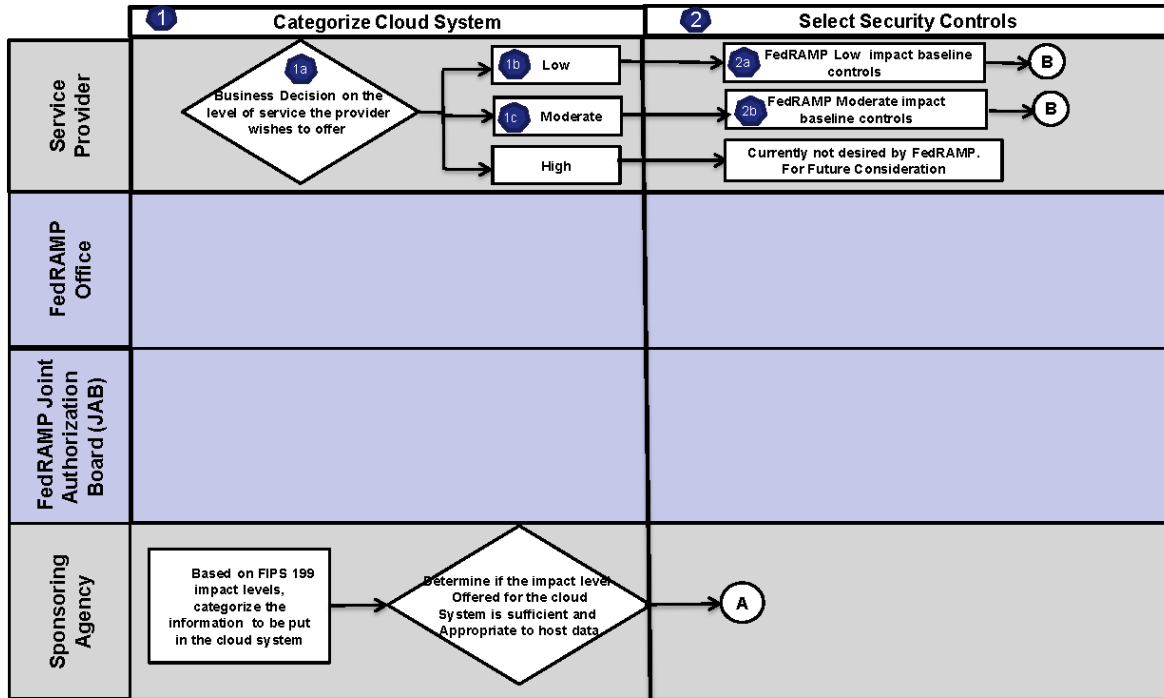
590 FedRAMP Assessment and Authorization is an effort composed of many entities/stakeholders  
591 working together in concert to enable government-wide risk management of cloud systems. The  
592 following diagrams describe the steps and workflow of the FedRAMP Assessment and  
593 Authorization process.



594

595 **Figure 6: FedRAMP Assessment and Authorization Process**

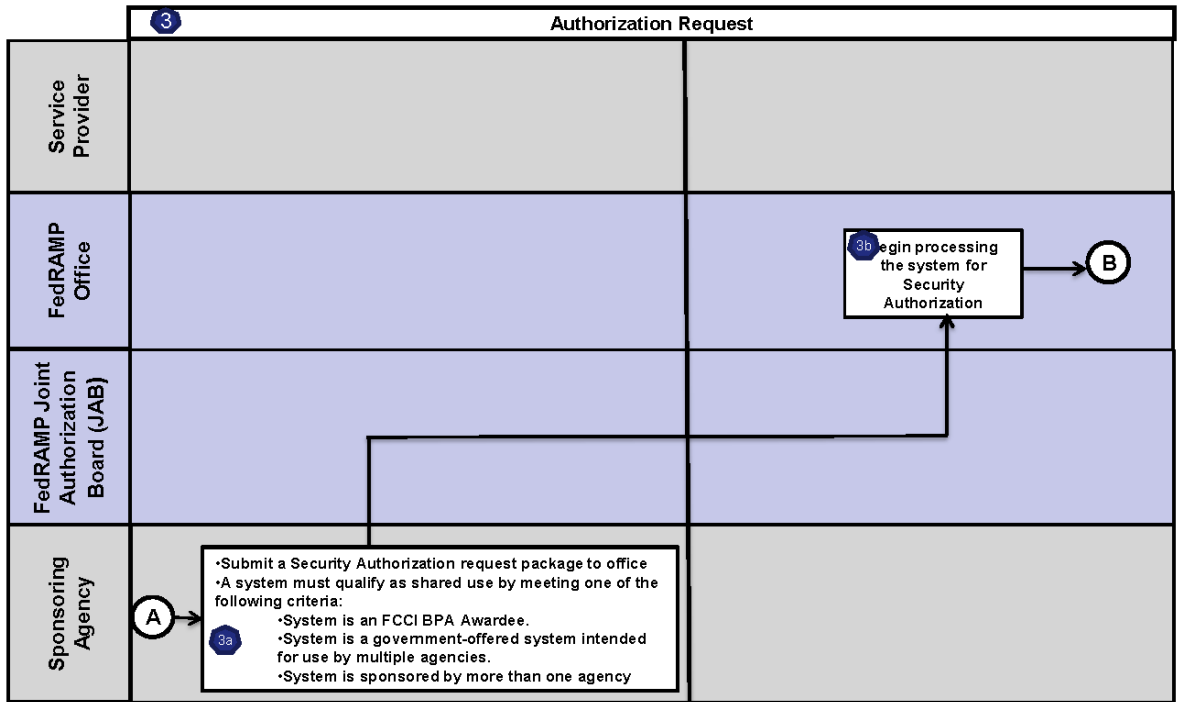
## FedRAMP – Categorize Cloud System and Select Security Controls



596  
597

Figure 7: FedRAMP Categorization of Cloud System and Select Security Controls

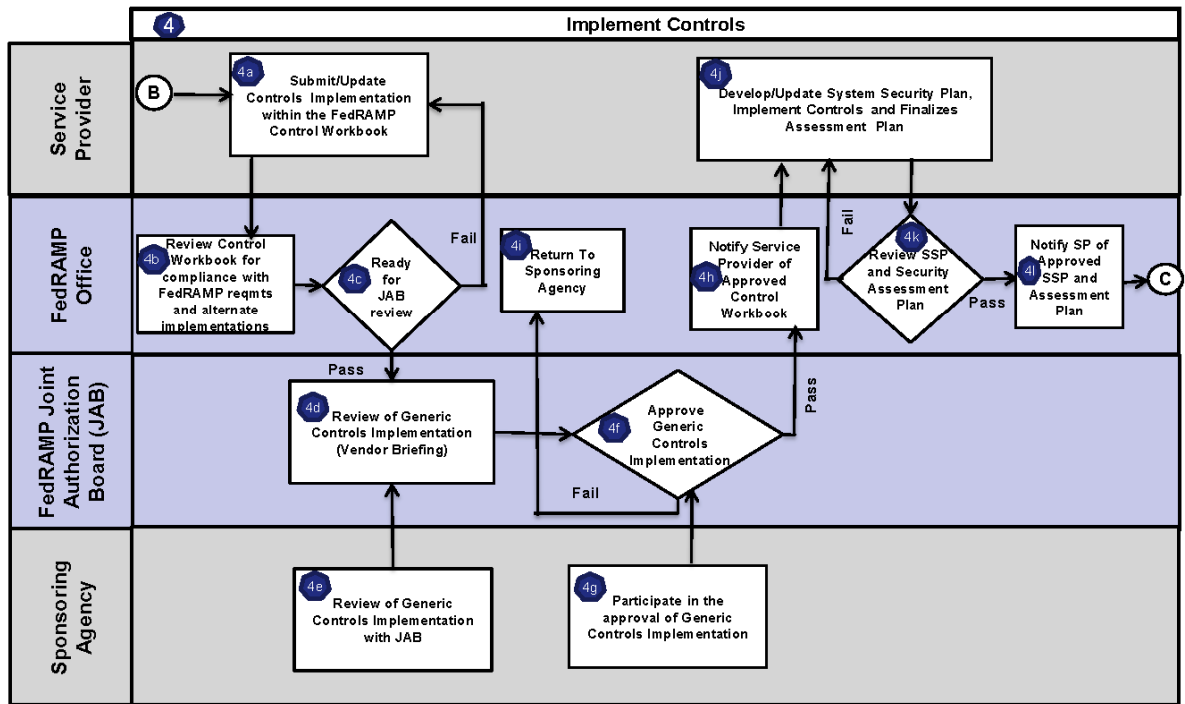
## FedRAMP – Authorization Request



598  
599

Figure 8: FedRAMP Authorization Request

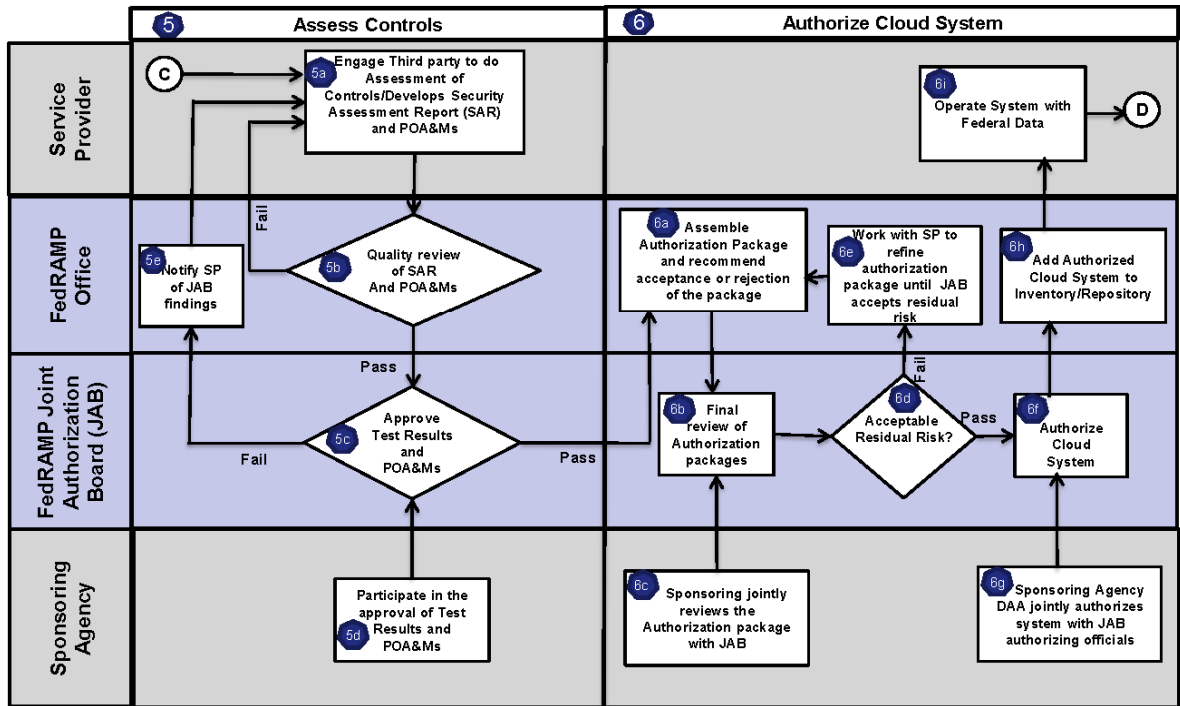
## FedRAMP – Implement Controls



600  
601

Figure 9: Implement Controls

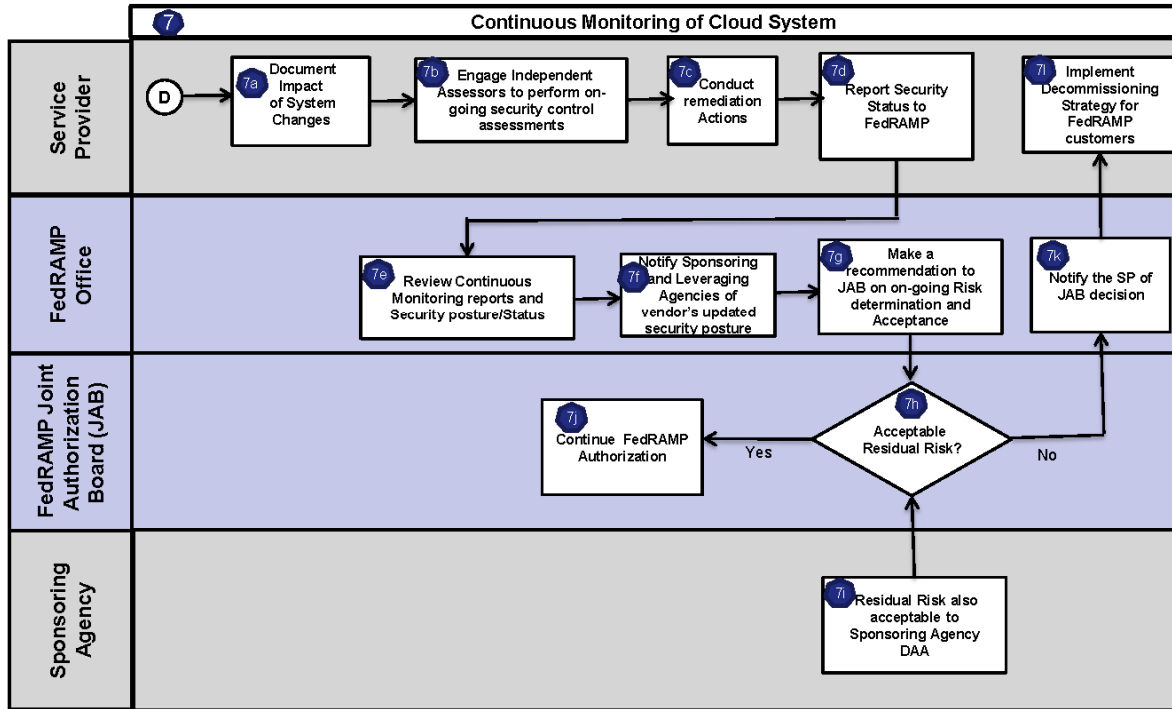
## FedRAMP – Assess Controls, Authorize Cloud System



602  
603

Figure 10: Assess Controls, Authorize Cloud System

## FedRAMP – Continuous Monitoring of Cloud System



604  
605

Figure 11: Continuous Monitoring

606 The following section provides the list of NIST special publications, FIPS publications, OMB  
607 Memorandums, FedRAMP templates and other guidelines and documents associated with the  
608 seven steps of the FedRAMP process:

609 **Step 1 - Categorize Cloud System:** (FIPS 199 / NIST Special Publications 800-30, 800-39,  
610 800-59, 800-60.)

611 **Step 2 – Select Security Controls:** (FIPS Publications 199, 200; NIST Special Publications  
612 800-30, 800-53 R3, FedRAMP security control baseline)

613 **Step 3 – Authorization Request:** (FedRAMP primary Authorization Request letter, FedRAMP  
614 secondary authorization request letter)

615 **Step 4 - Implement Controls:** (FedRAMP control tailoring workbook; Center for Internet  
616 Security (CIS); United States Government Configuration Baseline (USGCB); FIPS  
617 Publication 200; NIST Special Publications 800-30, 800-53 R3, 800-53A R1)

618 **Step 5 – Assess Controls:** (FedRAMP Test Procedures: Center for Internet Security (CIS);  
619 United States Government Configuration Baseline (USGCB); NIST Special  
620 Publication 800-53A R1)

621 **Step 6 – Authorize Cloud System:** OMB Memorandum 02-01; NIST Special Publications 800-  
622 30, 800-53A R1)

623 **Step 7 – Continuous Monitoring:** FedRAMP Test Procedures; NIST Special Publications  
624 800-30, 800-53A R1, 800-37 R1

625 A description of the process steps is listed in Table 4: FedRAMP Process Steps. The table is organized by step process families  
 626 relating to the aforementioned steps. The table provides the following information:

- 627 • **Process Step** – The distinct step in the process and divided into sub-steps identified with a letter appendix such as “1a”.
- 628 • **Description** – A high level description of the activities occurring with each step.
- 629 • **Deliverable** – A list of the deliverables associated with the steps if the step has any applicable deliverables. Where no  
 630 deliverable is expected, the table cell is blank.
- 631 • **Primary Responsibility** – The entity with the primary responsibility of executing/implementing the steps.
- 632 • **Notes/Instructions** – Specific comments on how the entity with primary responsible implements each step.

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
<b>1 Categorize Cloud System</b>				
1a, 1b, and 1c	Cloud Service Provider (CSP) makes a business decision of the security impact level (Low or Moderate) they wish to support or get authorized for their system/cloud offering.	<ul style="list-style-type: none"> <li>• Authorization request letter documenting FIPS 199 impact level to be supported by the cloud system.</li> </ul>	Cloud System Owner and Customer Agency	In this phase, the customer Agency is required to categorize the information/data to be put in the cloud and determine if the impact level offered by the CSP is sufficient and appropriate to host their Agency data.
<b>2 Select Security Controls</b>				
2a and 2b	<ul style="list-style-type: none"> <li>• If the CSP chooses to be authorized at Low impact level, they need to comply with the FedRAMP Low impact security control baseline (provided in Chapter 3)</li> <li>• If the CSP chooses to be authorized at Moderate impact level, they need to comply with the FedRAMP Moderate impact security control baseline (provided in Chapter 3)</li> </ul>		Cloud System Owner	In this phase, the Sponsoring Agency may add any agency-specific controls over the FedRAMP baseline.

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
<b>3 Authorization Request</b>				
3a and 3b	<ul style="list-style-type: none"> <li>Submit a Security Authorization request package to FedRAMP. A request package must include ALL of the following documents:                             <ol style="list-style-type: none"> <li>Authorization request letter from the requesting agency's CIO.</li> </ol> </li> <li>Once all documents are received, the "security authorization request" will be officially acknowledged and documented in request log and FedRAMP will begin processing the system for security authorization.</li> </ul>	<ul style="list-style-type: none"> <li>FedRAMP primary and secondary Authorization Request Letter (if applicable)</li> <li>Copy of Signed Contract</li> </ul>	Sponsoring Agency	<ul style="list-style-type: none"> <li><b>Verify multi-agency use of the system</b> In order to undergo FedRAMP Authorization, a system must qualify as shared use by meeting one of the following criteria:                             <ol style="list-style-type: none"> <li>System is an FCCI BPA Awardee.</li> <li>System is a government-offered system intended for use by multiple agencies.</li> <li>System is sponsored by more than one agency</li> </ol> </li> </ul>
<b>4 Implement Controls</b>				
4a	The service provider begins the FedRAMP authorization process by documenting generic controls implementation and defining the implementation settings for organization defined parameters and any compensating security controls as required by FedRAMP Control Tailoring Workbook	<ul style="list-style-type: none"> <li>FedRAMP Control Tailoring Workbook</li> <li>Control Implementation Summary table.</li> </ul>	Cloud Service Provider (CSP)	<ul style="list-style-type: none"> <li><i>Instruction:</i> Complete column G of the workbook and submit to FedRAMP for verification/approval as part of the initial SSP with sections 1-12 and select controls in section 13 completed.</li> </ul> <p>This is required before assessment activities can begin to assure agreement of organizational settings by the JAB</p> <ul style="list-style-type: none"> <li>All service providers must complete the Control Implementation Summary Table</li> </ul>

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
				<p><i>(Sample provided in FedRAMP Templates)-</i> which is customized for the service provider’s system and its environment. The completed table identifies controls types (common vs. hybrid controls vs. app specific controls) with implementation status (Fully Implemented, Partially Implemented, Not Implemented, Not Applicable) across all required controls. The service provider completed table must reflect controls based on NIST 800-53 R3 and provide status for both controls and enhancements (as applicable per FIPS 199 impact and FedRAMP required controls). The columns can and should be customized to the service providers’ environment to account for controls and minor apps (as necessary).</p>
4b	<p>FedRAMP reviews the Control Tailoring Workbook provided by the vendor for compliance with FedRAMP security requirements and acceptable risk criteria</p>			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
4c	FedRAMP determines if the Control Tailoring Workbook is ready for JAB review. If yes, then see 4d and 4e, otherwise FedRAMP sends the workbook back to the service provider to fix it.			
4d and 4e	JAB (consisting of DHS, DOD and GSA) and the Requesting/Sponsoring Agency receive a CSP/FedRAMP briefing on the generic control implementation. JAB and requesting Agency review the Control Tailoring Workbook for compliance and alternate implementations/compensating controls to determine effectiveness and make a risk-based decision.			<ul style="list-style-type: none"> <li>• <b>Instruction</b> - When the FedRAMP Control Tailoring Workbook and Control Summary have been completed and submitted to FedRAMP for review, FedRAMP may request a meeting with the Service Provider at this stage to review the documents or give the go-ahead to proceed with the authorization process.</li> </ul>
4f and 4g	JAB and the Requesting/sponsoring Agency jointly Approve/Reject the Control Tailoring Workbook and the decision to proceed further.			
4h	If approved, FedRAMP notifies the service provider of JAB approval and allow the vendor to proceed with the development of System Security Plan (SSP) and Assessment plan			
4i	If rejected, then FedRAMP notifies the requesting agency, which then asks the service provider to come for FedRAMP Authorization when they meet the FedRAMP requirements.			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
4j	If the Control Tailoring Workbook is approved, then service provider proceeds with the development of SSP, Assessment plan and implementation of the controls per SSP. Upon completion of SSP and Assessment plan, it is submitted to the FedRAMP for review.	<ul style="list-style-type: none"> <li>• System Security Plan (SSP)</li> <li>• Assessment Plan</li> </ul>		<ul style="list-style-type: none"> <li>• The FedRAMP security assessment test procedures, as located in reference materials, must be used as the basis for all security assessment and continuous monitoring activities.</li> <li>• <b>Instruction</b> - The FedRAMP must accept the System Security Plan and Security Assessment Plan before assessment activities can begin. System Security Plan and Security Assessment Plan should be submitted to the FedRAMP for review and approval at this time.</li> </ul>
4k	FedRAMP reviews the SSP and Assessment plan.			
4l	If satisfactory, then see 5a otherwise the SSP and/or Assessment plan are sent back to the service provider to fix the issues identified.			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
<b>5 Assess Controls</b>				
5a	<p>Upon approval of SSP and Assessment plan from FedRAMP, the service provider should engage third party independent assessor to assess the effectiveness of implemented controls using FedRAMP’s Assessment Procedures. The independent assessor documents the results of the assessment in the Security Assessment Report (SAR) using FedRAMP’s template. Any outstanding issues should be documented in the POA&amp;M’s. Both SAR and POA&amp;M are submitted to FedRAMP for review.</p>	<ul style="list-style-type: none"> <li>• Security Assessment Report (SAR)</li> <li>• POA&amp;M</li> <li>• Updated SSP</li> </ul>		<p>Service Provider Owner should update the system security plan based on the results of the risk assessment and any modifications to the security controls in the information system. Update the SSP to reflect the actual state of the security controls implemented in the system following completion of security assessment activities.</p>
5b	<p>FedRAMP reviews the test results documented in the SAR and any outstanding issues in the POA&amp;M to determine if the documented risk seems acceptable for JAB. FedRAMP repeats this process with the CSP until the documents are acceptable. Once they are acceptable, then FedRAMP provides these documents to the JAB including the requesting Agency with a summary of the results in the documents.</p>			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
5c and 5d	JAB and the requesting agency review the test results and POA&M's. If the test results demonstrate that the security controls are effectively implemented and if the outstanding issues in the POA&M are acceptable, then the JAB notifies FedRAMP of their approval and the process moves to Step 6a.			
5e	However, JAB may have questions/concerns associated with the test results or outstanding issues. FedRAMP communicates these with the CSP in this step.			
<b>6 Authorize Cloud System</b>				
6a	FedRAMP assembles the authorization package based on the updated deliverables received from the CSP to this point and makes a recommendation of acceptance or rejection of the package to the JAB	<ul style="list-style-type: none"> <li>Complete CSP authorization package</li> </ul>	FedRAMP and CSP	
6b and 6c	JAB including the requesting/sponsoring Agency performs a final review of the CSP authorization package			
6d	Based on the review in steps 6b and c, make a determination on the acceptance or rejection of the residual risk.			

Process Step	Description	Deliverable (if applicable)	Primary responsibility	Notes/Instructions
6e	If rejected, then FedRAMP works with the CSP to refine the package until the residual risk in the cloud system is acceptable to the JAB			
6f and 6g	If accepted, then the JAB including the requesting/sponsoring Agency issues the Authority To Operate the cloud system			
6h	FedRAMP authorized systems are added to a repository of authorized systems that can be leveraged by other Federal Agencies			
6i	The cloud system is operational with Federal data processed on the system			
<b>7 Continuous Monitoring</b>				More details about the FedRAMP Continuous Monitoring phase can be found in Chapter 2: Continuous Monitoring.

633 **Table 4: FedRAMP Process Steps**

634 **3.4.2.5. Risk Acceptability Criteria**

635 The following table lists the FedRAMP JAB acceptable risk criteria. In particular the table lists  
 636 the “Not Acceptable” risk criteria and the ones requiring JAB prior approval.

Not Acceptable	Requires JAB Prior Approval
<ul style="list-style-type: none"> <li>• Vulnerability Scanner output has HIGH vulnerabilities not remediated.</li> <li>• More than 5% of total security controls are reflected within the POA&amp;M.</li> <li>• False Positive claims are not supported by evidence files.</li> <li>• FedRAMP audit shows configuration, which differs from presented documentation.</li> <li>• OS out of lifecycle Support (Windows XP and before).</li> <li>• Hot fix patches not implemented, without justification</li> <li>• Does not support 2-factor authentication from customer agency to cloud for moderate impact system. Does not support FIPS 140-2 from customer agency to the cloud.</li> </ul>	<ul style="list-style-type: none"> <li>• Change in inter-connections.</li> <li>• Change in ISA/MOU.</li> <li>• Change in physical location.</li> <li>• Change in Security Impact Level.</li> <li>• Threat Changes.</li> <li>• Privacy Act security posture change.</li> <li>• OS Change (2K to 2K3, Windows to Linux, etc).</li> <li>• Change in SW (i.e. Oracle to SQL).</li> </ul>

637 **Table 5: FedRAMP Risk Acceptability Criteria**

638 **3.5. Authorization Maintenance Process**

639 Once a system has received a FedRAMP authorization, several events take place. First, the  
 640 system is added to the FedRAMP online repository of authorized systems. Next, FedRAMP will  
 641 begin facilitating agency access to the approved authorization package to enable agency review  
 642 of the material. Lastly, FedRAMP will begin overseeing continuous monitoring of the system  
 643 and advise the JAB of any changes to risk posture.

644 FedRAMP will maintain an online repository of cloud system authorizations in two categories:

- 645 • Authorizations granted by the JAB
- 646 • Authorizations granted by individual Agencies

647 This web based resource will be publicly accessible and will be the authoritative source of  
 648 FedRAMP system authorization status. The web based resource will maintain the following  
 649 information for each currently authorized system.

- 650 • System Name and scope of authorization (examples of scope include IaaS, PaaS or SaaS,  
 651 entire or partial suite of products offered by CSP)
- 652 • FIPS 199 impact level supported by the cloud system
- 653 • Expiration date for Authorization
- 654 • Version of FedRAMP requirements and templates used to authorize the system

- 655 • Points of Contact for the cloud system

656 FedRAMP will also maintain a secure website (separate from the public website) accessible only  
657 to Federal officials to access CSP authorization packages and communicate cloud system  
658 specific updates on the risk posture.

### 659 **3.6. Authorization Leveraging Process**

660 The purpose of all of the FedRAMP authorizations is to facilitate the leveraging of these  
661 authorizations for use by multiple federal agencies (“Approve once. Use often”). Leveraging  
662 such authorizations is employed when a federal agency chooses to accept all of the information  
663 in an existing authorization package via FedRAMP.

664 A FedRAMP joint authorization is not a “Federal Authority to Operate” exempting Federal  
665 Agencies, Bureaus, and Divisions from individually granting Authorities to Operate. A  
666 FedRAMP Authorization provides a baseline Authorization for Federal Agencies, Bureaus, and  
667 Divisions to review and potentially leverage. As is consistent with the traditional authorization  
668 process, an authorizing official in the leveraging organization is both responsible and  
669 accountable for accepting the security risks that may impact the leveraging organization’s  
670 operations and assets, individuals, other organizations, or the Nation.

671 The leveraging organization reviews the FedRAMP authorization package as the basis for  
672 determining risk to the leveraging organization. When reviewing the authorization package, the  
673 leveraging organization considers risk factors such as the time elapsed since the authorization  
674 results were produced, the results of continuous monitoring, the criticality/sensitivity of the  
675 information to be processed, stored, or transmitted, as well as the overall risk tolerance of the  
676 leveraging organization.

677 FedRAMP will provide leveraging agencies with access to the authorization packages to assist in  
678 their risk management decision. If the leveraging organization determines that there is  
679 insufficient information in the authorization package or inadequate security measures in place for  
680 establishing an acceptable level of risk, the leveraging organization needs to communicate that to  
681 FedRAMP. If additional information is needed or additional security measures are needed such  
682 as increasing specific security controls, conducting additional assessments, implementing other  
683 compensating controls, or establishing constraints on the use of the information system or  
684 services provided by the system these items will be facilitated by FedRAMP. The goal is to keep  
685 unique requirements to a minimum, but consider any other additional security controls for  
686 implementation and inclusion in the baseline FedRAMP security controls.

687 The leveraged authorization approach provides opportunities for significant cost savings and  
688 avoids a potentially costly and time-consuming authorization process by the leveraging  
689 organization. Leveraging organizations generate an authorization decision document and  
690 reference, as appropriate, information in the authorization package from FedRAMP.

691 All of the FedRAMP authorizations do not consider the actual information placed in the system.  
692 It is the leveraging agencies responsibility to do proper information categorization and  
693 determination if privacy information will be properly protected and if a complete Privacy Impact  
694 Assessment is in place. In almost all cases the FedRAMP authorization does not consider the  
695 actual provisioning of users and their proper security training. In all cases additional security  
696 measures will need to be documented. The leveraging organization documents those measures

697 by creating an addendum to the original authorization package of FedRAMP or a limited version  
698 of a complete package that references the FedRAMP authorization. This addendum may  
699 include, as appropriate, updates to the security plan (for the controls that is customer Agency's  
700 implementation responsibility), security assessment report, and/or leveraging organization's plan  
701 of action and milestones. FedRAMP will report the base system for FISMA purposes and the  
702 leveraging agency will need to report their authorization via their organizational FISMA process.

703 Consistent with the traditional authorization process, a single organizational official in a senior  
704 leadership position in the leveraging organization is both responsible and accountable for  
705 accepting the information system-related security risks that may impact the leveraging  
706 organization's operations and assets, individuals, other organizations, or the Nation.

707 The leveraged authorization remains in effect as long as the leveraging organization accepts the  
708 information system-related security risks and the authorization meets the requirements  
709 established by federal and/or organizational policies. This requires the sharing of information  
710 resulting from continuous monitoring activities conducted by FedRAMP and will be provided to  
711 agencies that notify FedRAMP that they are leveraging a particular package. The updates will  
712 include such items as updates to the security plan, security assessment report, plan of action and  
713 milestones, and security status reports. To enhance the security of all parties, the leveraging  
714 organization can also share with the owning organization, the results from any RMF-related  
715 activities it conducts to supplement the authorization results produced by the owning  
716 organization.

### 717 **3.7. Communications Process**

718 FedRAMP interacts with multiple stakeholders during the security lifecycle of a system. To  
719 streamline the workflow, a secure website is under development to facilitate updates on status,  
720 provide secure posting of artifacts and provide baseline information. However, in addition to  
721 this online web portal, proactive communication is required to ensure the success of each  
722 individual cloud system authorization. It is expected that the Cloud Service Providers,  
723 FedRAMP and Sponsoring and Leveraging Agencies will communicate regularly to ensure that  
724 information is disseminated effectively.

725 The following communication templates will be employed:

- 726 • Sponsorship Letter
- 727 • Status Report
- 728 • Confirmation Receipts (Complete Package, Incomplete Package)
- 729 • Review Recommendation (Acceptable, Unacceptable)
- 730 • Missing Artifact List
- 731 • Incident Report

732 The communication plan in Table 6: Communications Plan identifies the touch points and how  
733 communication will be delivered between FedRAMP, Leveraging Agencies, Sponsoring  
734 Agencies, and the Cloud Service Providers. Additional emails, conference calls and in-person  
735 meetings to facilitate the process as the team deems necessary may augment the communication  
736 plan. As changes are integrated into the requirement process, the communication plan may be  
737 updated to respond to required changes to the communication process. At a minimum, the

738 communication plan will be reviewed annually. The table is organized by phases and depicts  
739 the communication flow in the following areas:

- 740 • **Trigger Event** – Identifies the event that will start the require communication during the  
741 different operational processes of FedRAMP
- 742 • **Deliverable** –Artifact used to communicate the results/output of the trigger event to  
743 FedRAMP stakeholders
- 744 • **Initiator** – The entity responsible for starting the communication process.
- 745 • **Target Audience** – Receivers of the deliverable in the communication process.
- 746 • **Delivery Method** – How the artifacts will be communicated to the target audience.

#	Trigger Event	Deliverable	Initiator	Target Audience	Delivery Method
Authorization Request, Assessment and Authorization Phases					
1	Initiation of FedRAMP A&A Process	Sponsorship Letter, Contract	Sponsoring Agency	FedRAMP	Upload through FedRAMP Website
2	Receipt of Sponsorship Letter	Kickoff Meeting	FedRAMP	Sponsoring Agency, Cloud Service Provider	Scheduled with the participants identified through the sponsorship letter, this first meeting will allow the participants an opportunity to understand the process and establish milestone dates.
3	Weekly Status Report	Status Report	FedRAMP	Sponsoring Agency, Cloud Service Provider	Uploaded to Secure Web Portal, the status report is updated weekly advising of current status and future target dates.
4	Questions about requirements	Email Inquiry	Cloud Service Provider	FedRAMP	Cloud Service Provider may email questions to FedRAMP.
5	Received Questions	Email Clarification	FedRAMP	Cloud Service Provider	FedRAMP will respond to email questions within two business days.
6	Package Submission	Completed Artifact(s)	Cloud Service Provider	FedRAMP	Securely uploaded through FedRAMP Website.
7	Completed Package Submission	Confirmation Receipt – Completed Package	FedRAMP	Cloud Service Provider	Emailed acknowledgement receipt by FedRAMP Review Team identifies the received artifacts and target date for completed review.

#	Trigger Event	Deliverable	Initiator	Target Audience	Delivery Method
8	Incomplete Package Submission	Confirmation Receipt – Incomplete Package	FedRAMP	Cloud Service Provider	Emailed acknowledgement receipt by FedRAMP Review Team identifies which artifacts have been received and which are still missing.
9	FedRAMP completes artifact review, recommends ATO	Review Recommendation	FedRAMP	JAB, Sponsoring Agency, Cloud Service Provider	Emailed recommendation explains the Cloud Service Provider’s compliance with the required risk management controls.
10	FedRAMP completes artifact review, recommends improvements	Review Recommendation	FedRAMP	Cloud Service Provider	Emailed Review Recommendation includes individual areas of focus required by the Cloud Service Provider to be compliant with FedRAMP requirements.
11	Completed review, improvements recommended	Findings Review Meeting	FedRAMP	Sponsoring Agency, Cloud Service Provider	Scheduled by FedRAMP, this meeting allows the Cloud Service Provider and the Sponsoring Agency an opportunity to discuss and understand any deficiencies identified by the FedRAMP review team.
Authorization Maintenance Phase					

#	Trigger Event	Deliverable	Initiator	Target Audience	Delivery Method
12	FedRAMP authorizes system	Joint Authorization Letter	JAB, FedRAMP	Cloud Service Provider, Sponsoring Agency, Leveraging Agency	<p>Post the following information on a public FedRAMP website about the authorized system:</p> <ul style="list-style-type: none"> <li>System Name</li> <li>FIPS 199 impact level the system is authorized at</li> <li>Version of FedRAMP security controls and other templates used</li> <li>Authorization Expiration Date</li> <li>Privacy Questionnaire</li> </ul> <p>Maintain the authorization package including but not limited to SSP, SAR, Contingency Plan, Incident reporting plan, POA&amp;M's on a secure website accessible by Government officials only</p>
13	Granting authorization package access to leveraging Agencies	CSP Authorization Package	FedRAMP	Leveraging Agency	Provide secure access (login) to Government-only website for accessing CSP authorization package
Continuous Monitoring Phase					

#	Trigger Event	Deliverable	Initiator	Target Audience	Delivery Method
14	Creation of updated artifacts (e.g. SSP, POA&M's)	Updated Artifacts	Cloud Service Provider	FedRAMP	Uploaded to Secure Web Portal, the Cloud Service Provider will post all regular recurring artifacts for FedRAMP team review.
15	Receipt of Updated Artifacts	Confirmation Receipt	FedRAMP	Cloud Service Provider	Email acknowledgement receipt of uploaded artifacts.
16	Accepted Artifacts	Review Recommendation – Acceptable	FedRAMP	Leveraging Agencies, Cloud Service Provider	Update on secure website that Cloud Service Providers updated artifacts meet compliance requirements.
17	Unacceptable Artifacts	Review Recommendation - Unacceptable	FedRAMP	Leveraging Agencies, Cloud Service Provider	Email Notification of what issues the Cloud Service Provider is required to remediate to remain within compliance. Update on Secure Web Site identifying outstanding issues.
18	Updated Artifacts not received with 1 week of due date	Missing Artifact List	FedRAMP	Cloud Service Provider	Email Notification to the Cloud Service Provider that their artifacts have not been received.
17	Updated Artifacts not received with 2 weeks of due date	Missing Artifact List	FedRAMP	Leveraging Agencies, Cloud Service Provider	Email Notification to the Cloud Service Provider that their artifacts have not been received and their ATO is at risk.
18	Incident	Incident Reporting/Notification	Cloud Service Provider	Leveraging Agencies, FedRAMP	

747 [Table 6: Communications Plan](#)

## 748 3.8. Change Management Process

749 The technology changes within the dynamic and scalable cloud computing environment are  
750 expected to be quite swift. As the cloud computing market matures, best practices associated  
751 with the implementation and testing of security controls will evolve.

752 There are multiple industry groups, academic collaborations, engineering teams, policy firms and  
753 assorted cadre of experts striving to maximize the potential of cloud computing in a secure  
754 environment. It is therefore obvious that FedRAMP will maintain resources to keep abreast of  
755 the technological and security enhancements in near real time. As these cloud computing best  
756 practices evolve, FedRAMP security requirements, processes and templates will also under go an  
757 evolution. The following sections define the FedRAMP change management process.

### 758 3.8.1. Factors for change

759 The following internal and external factors will drive the change to FedRAMP security  
760 requirements, processes and templates.

- 761 • ***Update to NIST special publications and FIPS publications:*** FedRAMP templates and  
762 requirements are based on the NIST special publications and FIPS publications. If the  
763 NIST SP 800-53 r3 is updated with new security controls and enhancements for low and  
764 moderate impact level, FedRAMP security controls will need to be updated. Also, if  
765 NIST publishes new guidance associated with cloud computing best practices, these will  
766 be considered for updates to FedRAMP security requirements and evaluation criteria/test  
767 procedures.
- 768 • ***Requirements from other Federal security initiatives:*** Government-wide security  
769 initiatives and mandates such as Trusted Internet Connections (TIC) and Identity,  
770 Credential and Access Management (ICAM) will drive updates to FedRAMP  
771 requirements for wider adoption of cloud computing systems and services across the  
772 Government. As the solutions for various cloud service models (IaaS, PaaS, SaaS), which  
773 is currently under active investigation, are adopted, they will be disseminated by  
774 FedRAMP. FedRAMP and the JAB will rely on both ISIMC and NIST to recommend  
775 changes to security controls over time. While these bodies will not have the authority to  
776 implement the changes, their expertise and reputation lend themselves to providing  
777 invaluable assistance to FedRAMP. It should be noted that security requirements can  
778 ***only*** be approved for change by the JAB.
- 779 • ***Agency-Specific requirements beyond the FedRAMP baseline:*** Federal Agencies  
780 leveraging FedRAMP authorizations for use within their own Agencies may add specific  
781 additional security controls, conduct additional assessments, or require implementation of  
782 other compensating controls. The leveraging agencies should notify FedRAMP of these  
783 additional requirements. FedRAMP JAB will meet regularly to discuss any required  
784 updates and possible inclusion of these additional security measures to FedRAMP  
785 security controls baseline and assessment procedures/evaluation criteria. If different  
786 leveraging Agencies have added different requirements and additional security measures  
787 for the same cloud system, FedRAMP will maintain a list of these additions and may  
788 consider updating either the FedRAMP baseline for all cloud systems or just that specific

789 cloud system. In both cases, FedRAMP will assess these additional controls/measures  
790 during the continuous monitoring phase.

- 791 • **Industry best practices, development of standards or use of new tools/technology:**  
792 FedRAMP requirements may be updated to adopt new standards as they are created for  
793 cloud computing interoperability, portability and security. As cloud computing market  
794 matures and as industry develops new tools and technologies for automated and near real  
795 time monitoring of controls and automated mechanisms for exposing audit data to  
796 comply with regulatory requirements become available, FedRAMP processes will also be  
797 updated accordingly.
- 798 • **Changes to cloud service provider offering:** As new features and components are added  
799 to the cloud service provider offering, additional requirements and assessments might be  
800 necessary to ensure that robust security posture of the system is maintained.

### 801 3.8.2. Security Documents/Templates Change Control

802 All security document templates are to be considered “living documents”. Over time, as  
803 requirements change, methodologies evolve, or new technologies and threats present themselves,  
804 these documents will undergo some degree of modification. FedRAMP is solely responsible for  
805 implementing these changes. It should be noted that FedRAMP security document templates are  
806 designed to assist the user with proper documentation related to their authorization package.  
807 These also serve to provide a more uniform content collection method that aids the CSP and  
808 agencies with achieving authorization status for the cloud service offering. As changes are  
809 made, updated templates will be posted to the FedRAMP website with instructions related to use.

### 810 3.8.3. Requirements for Cloud Service Provider Change Control 811 Process

812 Once a requirement is approved, CSP’s have 30 days to develop and submit an implementation  
813 plan. CSP’s are responsible for implementing the plans. The implementation plan needs to  
814 define the actions that the CSP must perform in order to comply with the new requirement. In  
815 most cases the implementation of the new control will be implemented within the 30 day  
816 window. However, there may be instances where the implementation of the controls will require  
817 the CSP to add the control to the POAM sheet, with milestones, target date, and resource  
818 allocations documenting the future implementation due to the nature of the control itself.  
819 Furthermore, it is understood that, depending on the particular infrastructure related to the  
820 security control, that it might be necessary for the CSP to implement a compensating control.  
821 This control will accomplish the same goal as the new requirement. However, it accomplishes  
822 the goal in a different manner. All compensating controls must receive authorization from the  
823 JAB. When situations arise where the new requirement cannot be implemented on a system due  
824 to the legacy nature of the infrastructure, or in cases where the control itself will have a severely  
825 negative impact on the mission of the system, the CSP may request a waiver. Waivers, though  
826 rare, must be presented to the JAB for approval. Once the control change is implemented,  
827 FedRAMP is to be notified and the security control baseline will be adjusted and documented.

828 **3.8.4.Sponsoring Agency CCP**

829 Sponsoring federal agencies maintain their responsibility for establishing and maintaining their  
830 own internal change control process. Responsibilities related to the cloud computing service  
831 offering should be limited to the interconnection between the agency and the CSP, and the input  
832 to any change requests.

833

834

## Document Revision History

---

835

Date	Description	Version	Author
11/02/2010	Proposed Security Assessment & Authorization for U.S. Government Cloud Computing	0.96	Federal Cloud Computing Initiative

836