

Federal Risk and Authorization Management Program (FedRAMP)

Developing Your System Security Plan

November 28, 2012





Today's Webinar

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services.

- The goal of this webinar is review the System Security Plan (SSP) and provide the information and guidelines that you need to accurately document the FedRAMP controls and assemble a strong SSP that will meet FedRAMP review requirements.





System Security Plan (SSP) Overview

- Detailed description of Control Implementation, based on NIST SP 800-53, r3
- Global view of how the system is structured
- Identifies personnel in the organization that are responsible for system security
- Delineates control responsibility between the customer or vendor
- The SSP is the key document to moving the FedRAMP assessment process forward
- Putting together a well documented SSP can save a lot of time in moving through the process

System Security Plan
<Information System Name>, <Date>

FedRAMP System Security Plan (Template)



<Vendor Name>

<Information System Name>

<Versio 1.0>
October 15, 2012

Company Sensitive and Proprietary
For Authorized Use Only



Why Such a Long Document?

- SSP template is 352 pages long
- Long template required to assure the system and implementation of controls are properly documented
- Effort to produce a well documented SSP leads to a smooth process





SSP Document Organization

1. System Information and Scope Section 1 – Section 12

1.	Information System Name/Title	23
2.	Information System Categorization	23
2.1.	Information Types.....	23
2.2.	Security Objectives Categorization (FIPS 199).....	25
2.3.	E-Authentication Determination (E-Auth).....	26
3.	Information System Owner.....	27
4.	Authorizing Official	27
5.	Other Designated Contacts.....	27
6.	Assignment of Security Responsibility	28
7.	Information System Operational Status	29
8.	Information System Type.....	29
8.1.	Cloud Service Model.....	29
8.2.	Leveraged Provisional Authorizations.....	30
9.	General System Description.....	30
9.1.	System Function or Purpose	31
9.2.	Information System Components and Boundaries.....	31
9.3.	Types of Users	31
9.4.	Network Architecture.....	32
10.	System Environment	32
10.1.1.	Hardware Inventory	33
10.1.2.	Software Inventory.....	33
10.1.3.	Network Inventory	34
10.1.4.	Data Flow	36
10.1.5.	Ports, Protocols and Services	36
11.	System Interconnections	37
12.	Applicable Laws and Regulations.....	39



SSP Document Organization

2. Description of Control Implementation Section 13

13.7.2 User Identification and Authentication (IA-2)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

IA-2	Control Summary Information
Responsible Role:	
Parameter:	
Implementation Status (check all that apply): <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	
Control Origination (check all that apply): <input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing Provisional Authorization (PA) for <Information System Name>, <Date of PA>	
IA-2 What is the solution and how is it implemented?	



SSP Document Organization

3. Appendix of Supporting Documents Section 14





Describe Your System

Sections 1 – 11 Contain Description of your System

- Section 1 – Basic System Info
- System Name
- Unique Identifier

1. INFORMATION SYSTEM NAME/TITLE

This System Security Plan provides an overview of the security requirements for the <Information System Name> (<Information System Abbreviation>) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is an asset vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the <Information System Name> information system.

The security safeguards implemented for the <Information System Name> system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1-1. Information System Name and Title

Unique Identifier	Information System Name	Information System Abbreviation

Section 2 – Information System Categorization

- Overall System Categorization
- CSP Data Information Types

2. INFORMATION SYSTEM CATEGORIZATION

The overall information system sensitivity categorization is noted in the table that follows.

Table 2-1. Security Categorization

Low	<input type="checkbox"/>
Moderate	<input type="checkbox"/>
High	<input type="checkbox"/>

2.1. INFORMATION TYPES

This section describes how the information types used by the information system are categorized for confidentiality, integrity, and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed, and/or output from <Information System Name>. The selection of the information types is based on guidance provided by OMB Federal Enterprise Architecture Program Management Office Business Reference Model 2.0, and FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* which is based on NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

Table 2-2. Sensitivity Categorization of Information Types

Information Type	Confidentiality	Integrity	Availability

Section 2 – Information System Categorization

- Security Objective Categorization (High Water Mark)
- Select Security Baseline based on Impact Level

2.2. SECURITY OBJECTIVES CATEGORIZATION (FIPS 199)

Based on the information provided in Table 2-2, Information Types, for the **<Information System Name>** default to the high-water mark for the noted Information Types as identified in the table below.

Table 2-3. Security Impact Level

Security Objective	Low, Moderate or High
Confidentiality	
Integrity	
Availability	

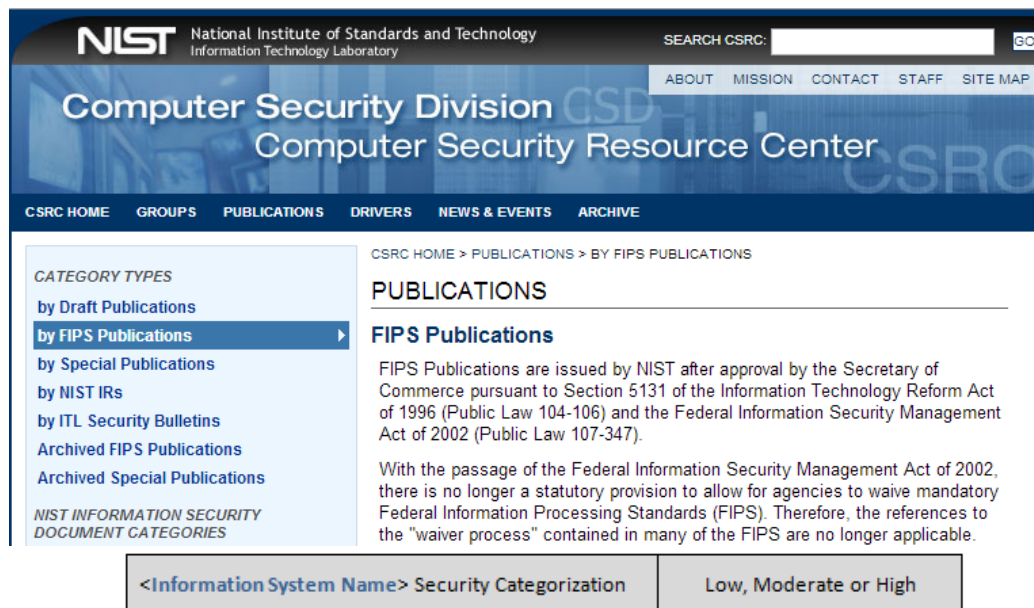
Table 2-4. Baseline Security Categorization

<Information System Name> Security Categorization	Low, Moderate or High
--	-----------------------

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

Section 2 – Information System Categorization

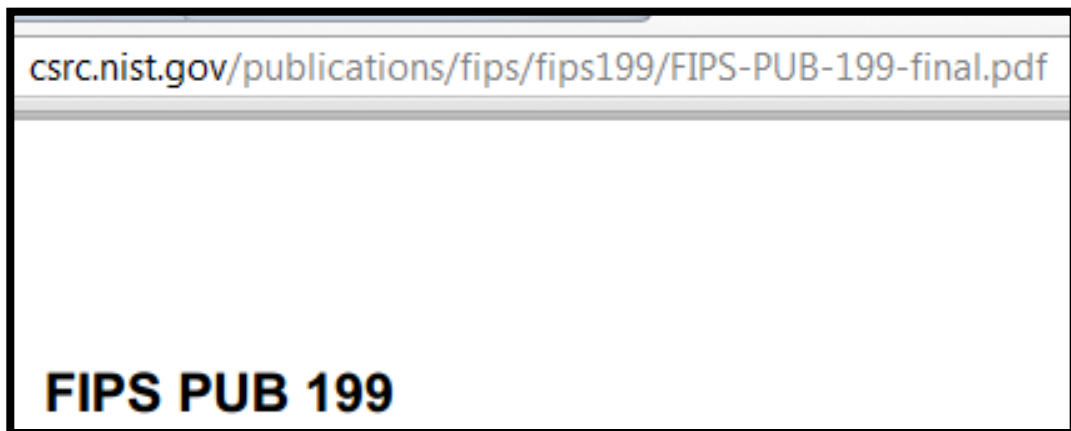
- FIPS Guidance on NIST CSRC Website



The screenshot shows the NIST Computer Security Division Computer Security Resource Center (CSRC) website. The header includes the NIST logo and navigation links. The main content area is titled "PUBLICATIONS" and features a sidebar with "CATEGORY TYPES" including "by Draft Publications", "by FIPS Publications" (selected), "by Special Publications", "by NIST IRs", "by ITL Security Bulletins", "Archived FIPS Publications", and "Archived Special Publications". The main text explains that FIPS Publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347). It also notes that with the passage of the Federal Information Security Management Act of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards (FIPS). Therefore, the references to the "waiver process" contained in many of the FIPS are no longer applicable.

Below the text, there is a table with two columns:

<Information System Name> Security Categorization	Low, Moderate or High
---	-----------------------



The screenshot shows the URL csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf in the browser address bar. Below the address bar, the document title "FIPS PUB 199" is displayed in large, bold, black text.



Section 2 – Selecting E-Authentication Level

- E-Authentication Determination

2.3. E-AUTHENTICATION DETERMINATION (E-AUTH)

The information system e-Authentication Determination is described in the table that follows.

Table 2-5. E-Authentication Questions

Yes	No	E-Authentication Question
<input type="checkbox"/>	<input type="checkbox"/>	Does the system require authentication via the Internet?
<input type="checkbox"/>	<input type="checkbox"/>	Is data being transmitted over the Internet via browsers?
<input type="checkbox"/>	<input type="checkbox"/>	Do users connect to the system from over the Internet?

Instruction: Any information system that has a "No" response to any one of the three questions does not need an E-Authentication risk analysis or assessment. For a system that has a "Yes" response to all of the questions, complete the E-Authentication Plan (a template is available).

Note: Please refer to *OMB Memo M-04-04 E-Authentication Guidance for Federal Agencies* for more information on e-Authentication.

The summary E-Authentication Level is recorded in the table that follows.


Table 2-6. E-Authentication Level Determination

E-Authentication Determination	
System Name	
System Owner	
Assurance Level	
Date Approved	



Section 2 – Selecting E-Authentication Level

- OMB Memo M-04-04, *EAuthentication Guidance for Federal Agencies*

 www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf



THE DIRECTOR

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 16, 2003

M-04-04

MEMORANDUM TO THE HEADS OF ALL DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

A handwritten signature of Joshua B. Bolten in black ink.

SUBJECT: E-Authentication Guidance for Federal Agencies



Section 3 -System Owner

- System Owner Contact

3. INFORMATION SYSTEM OWNER

The following individual is identified as the system owner or functional proponent/advocate for this system.

Table 3-1. Information System Owner

Name	
Title	
Company / Organization	
Address	
Phone Number	
Email Address	

Section 5 – Designated Contacts

- Technical and Management POC

5. OTHER DESIGNATED CONTACTS

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.



Table 5-1. Information System Management Point of Contact

Name	
Title	
Company / Organization	
Address	
Phone Number	
Email Address	

Table 5-2. Information System Technical Point of Contact

Name	
Title	
Company / Organization	
Address	
Phone Number	
Email Address	



Section 6 – Security Responsibility

- Information System Security Contact
- PMO will provide FedRAMP ISSO info

6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

or



Table 6-1. CSP Internal ISSO (or Equivalent)

Name	
Title	
Company / Organization	
Address	
Phone Number	
Email Address	

Table 6-2. FedRAMP Appointed ISSO

Name	
Title	FedRAMP ISSO
FedRAMP	
Address	1275 First Street, NE, Washington, DC, 20002, Room 1180
Phone Number	
Email Address	

Section 7– Operational Status

- List the operational state of the system

7. INFORMATION SYSTEM OPERATIONAL STATUS

The system is currently in the life-cycle phase noted in the table that follows.

Table 7-1. System Status

System Status		
<input type="checkbox"/>	Operational	The system is operating and in production.
<input type="checkbox"/>	Under Development	The system is being designed, developed, or implemented
<input type="checkbox"/>	Major Modification	The system is undergoing a major change, development, or transition.
<input type="checkbox"/>	Other	Explain:

Section 8 – Information System Type

- List cloud service model

8.1. CLOUD SERVICE MODEL

Information systems, particularly those based on cloud architecture models, are made up of different service layers. The layers of the <Information System Name> that are defined in this SSP, and are not leveraged by any other Provisional Authorizations, are indicated in the table that follows.

Instruction: Check all layers that apply.



Table 8-1. Service Layers Represented in this SSP

Service Provider Architecture Layers		
<input type="checkbox"/>	Software as a Service (SaaS)	Major Application
<input type="checkbox"/>	Platform as a Service (PaaS)	Major Application
<input type="checkbox"/>	Infrastructure as a Service (IaaS)	General Support System
<input type="checkbox"/>	Other	Explain:

Note: Please refer to *NIST SP 800-145* for information on cloud computing architecture models.



Section 8 –Information System Type

- Is the cloud service built on top of another cloud system with a FedRAMP Provisional ATO?

8.2. LEVERAGED PROVISIONAL AUTHORIZATIONS

Instruction: The FedRAMP program qualifies different service layers for Provisional Authorizations. One, or multiple service layers, can be qualified in one System Security Plan. See the section on Use Cases in Guide to Understanding FedRAMP for more information. If a lower level layer has been granted a Provisional Authorization, and another higher level layer represented by this SSP plans to leverage a lower layer's Provisional Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Provisional Authorizations, write "None" in the first column of the table that follows. Add as many rows as necessary in the table that follows.

The <Information System Name> <plans to/does not plan to> leverage a pre-existing Provisional Authorization. Provisional Authorizations leveraged by this <Information System Name> are noted in the table that follows.

Table 8-2. Leveraged Authorizations

Information System Name	Service Provider Owner	Date Granted

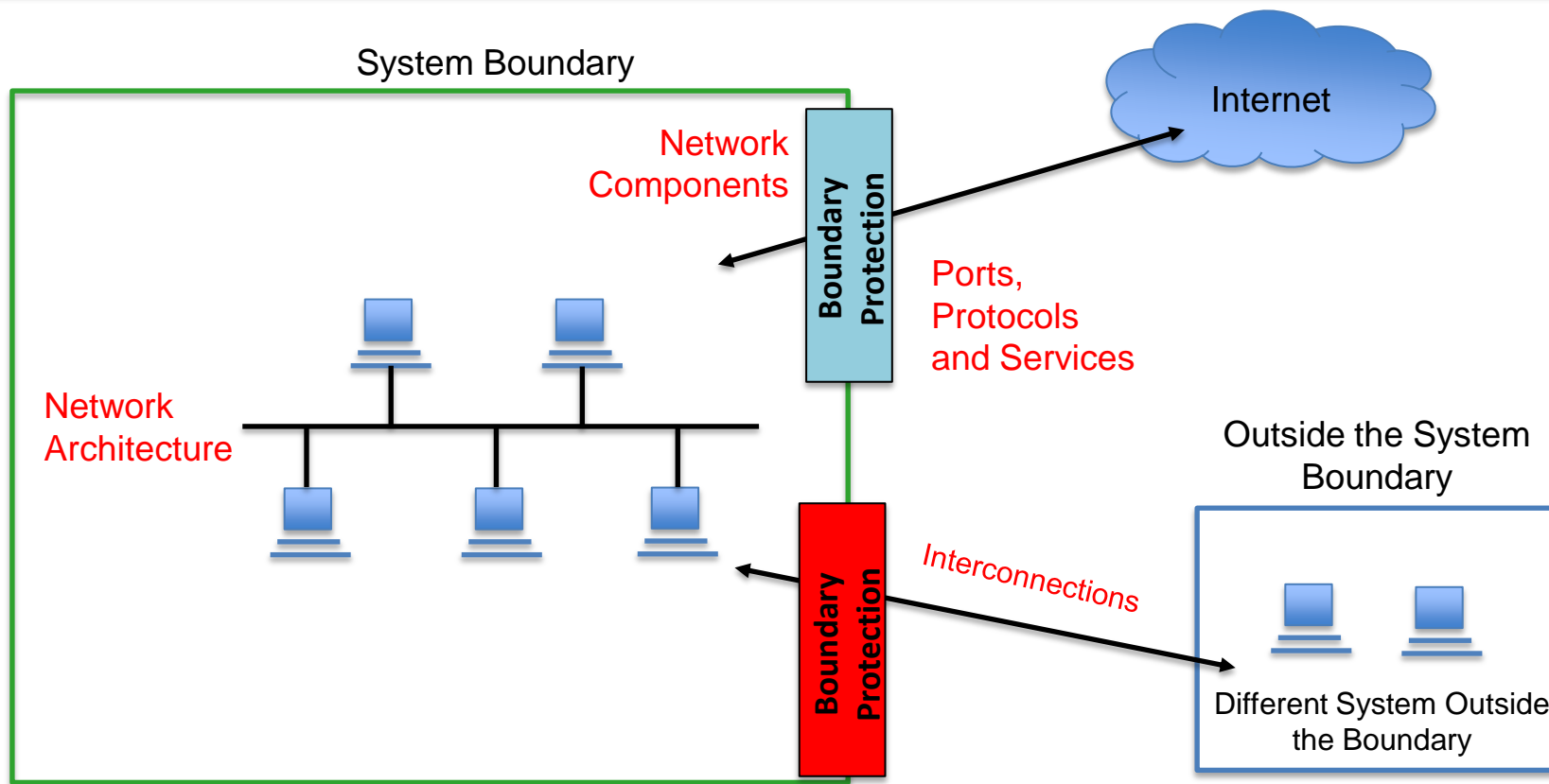
Note: Please refer to *NIST SP 800-145* for information on cloud computing architecture models.



Section 9 – General System Description

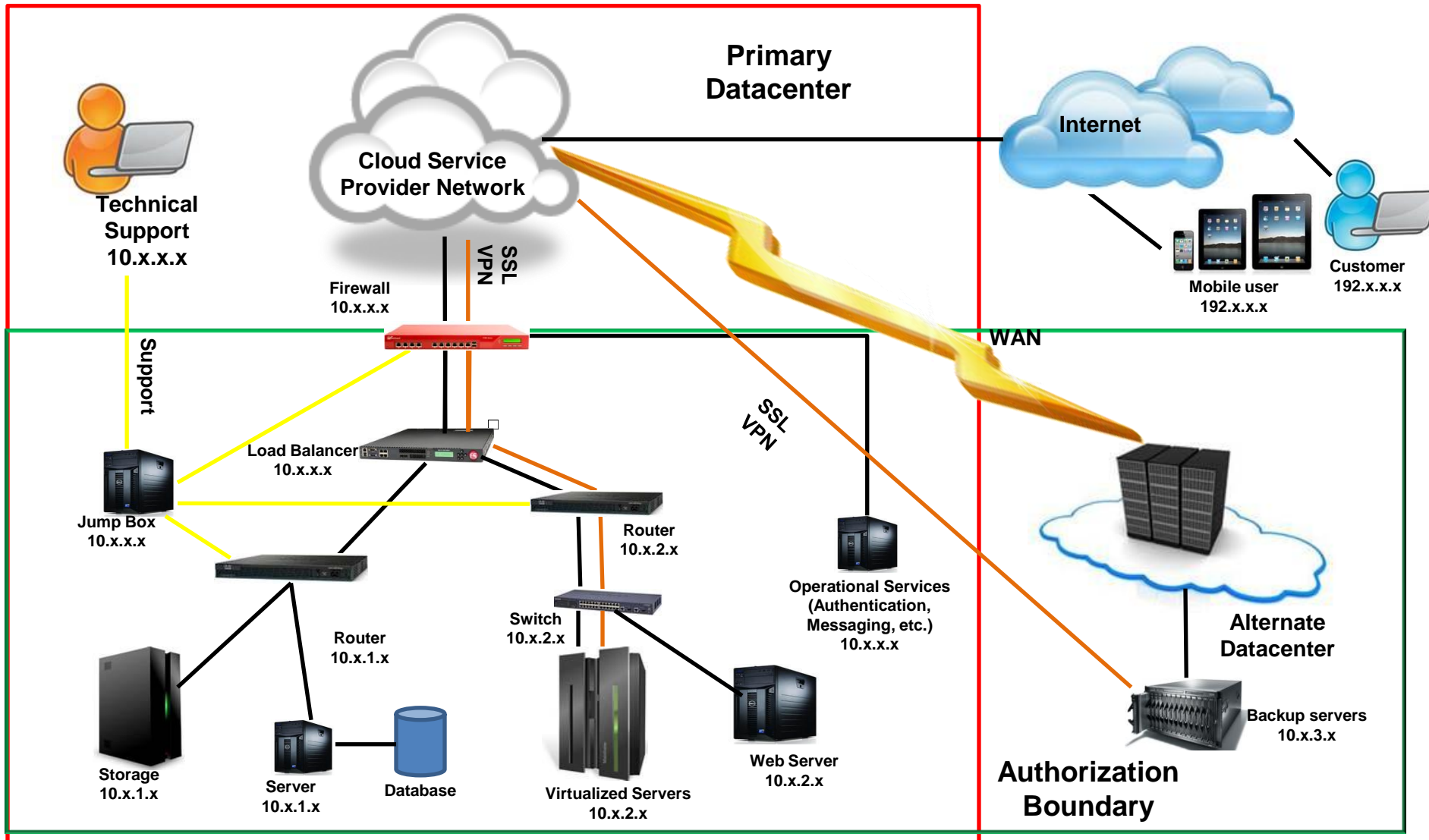
- The general System Description section contains some of the most important parts of the SSP in terms of defining the roles of the system's users, defining the system boundary, and describing the system architecture
- What is the purpose of the system?
 - Why was it built? What problem does it solve? What solution does it provide?
- Types of Users
 - Defined by what privileges the user is authorized to use
 - Is the user internal or external
 - Examples of roles include systems administrators, database administrators, release engineers, and customers
 - List other roles that have the ability to configure components that may affect services (web server administrators, network administrators, and firewall administrators)

Describing System Boundaries



- Understand which IT assets fit within the boundary.
- Interconnections: indicate and label interconnections to other systems
- Make sure your boundary is consistent with hardware & software inventory
- Make sure your diagrams are consistent with boundary descriptions

Describing the Network Architecture



Section 10 – System Environment

- System Inventories
 - Hardware

Table 10-1. Server Hardware Components

Hostname	Make	Model and Firmware	Location	Components that Use this Device
hostname1.com	Company	SilverEdge M710, 4.6ios	Dallas, Rm. 6, Rack 4	AppOne, EAuthApp
hostname2.com	Company	SilverEdge M610, 4.6ios	Datacenter2, Rack 7	VMs 1-50
Not Applicable	Company	iSCSI SAN Storage	Bldg 4, Rm 7	SAN Storage

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 3 CM-2.

Section 10 – System Environment

- System Inventories
 - Software

10.1.2. Software Inventory

The following table lists the principle software components for <Information System Name>.

Instruction: Please include any middleware, databases, or secure file transfer applications in this table. The first three rows are sample entries. The first three rows are sample entries. Add additional rows as needed.

Table 10-2. Software Components

Hostname	Function	Version	Patch Level	Virtual (Yes / No)
hostname1.com	Physical Host for Virtual Infrastructure	XYZI.4.x vSphere	Update 1	No
hostname2.com	Virtual Machine Application Server	Windows 2003 Server	SP2	Yes
hostname3.com	Virtual Database SQL Server	6.4.22 build 7	SP1	Yes

Section 10 – System Environment

- System Inventories
 - Network

10.1.3. Network Inventory

The following table lists the principle network devices and components for <Information System Name>.

Instruction: Please include any switches, routers, hubs, and firewalls that play a role in protecting the information system, or that enable the network to function properly. The first three rows are sample entries. If all network devices and components are leveraged from a pre-existing Provisional Authorization, write "Leveraged" in the first column. Add additional rows as needed.

Table 10-3. Network Components

Hostname	Make	Model	IP Address	Function
router-dallas	RouterCo	2800	192.168.0.1	router
switch-1	SwitchCo	EZSX55W	10.5.3.1	switch
fw.yourcompany.com	FirewallCo	21400, R71.x	192.168.0.2	firewall

Section 10 – System Environment

- System Inventories
 - Port, Protocols and Services

10.1.5. Ports, Protocols and Services

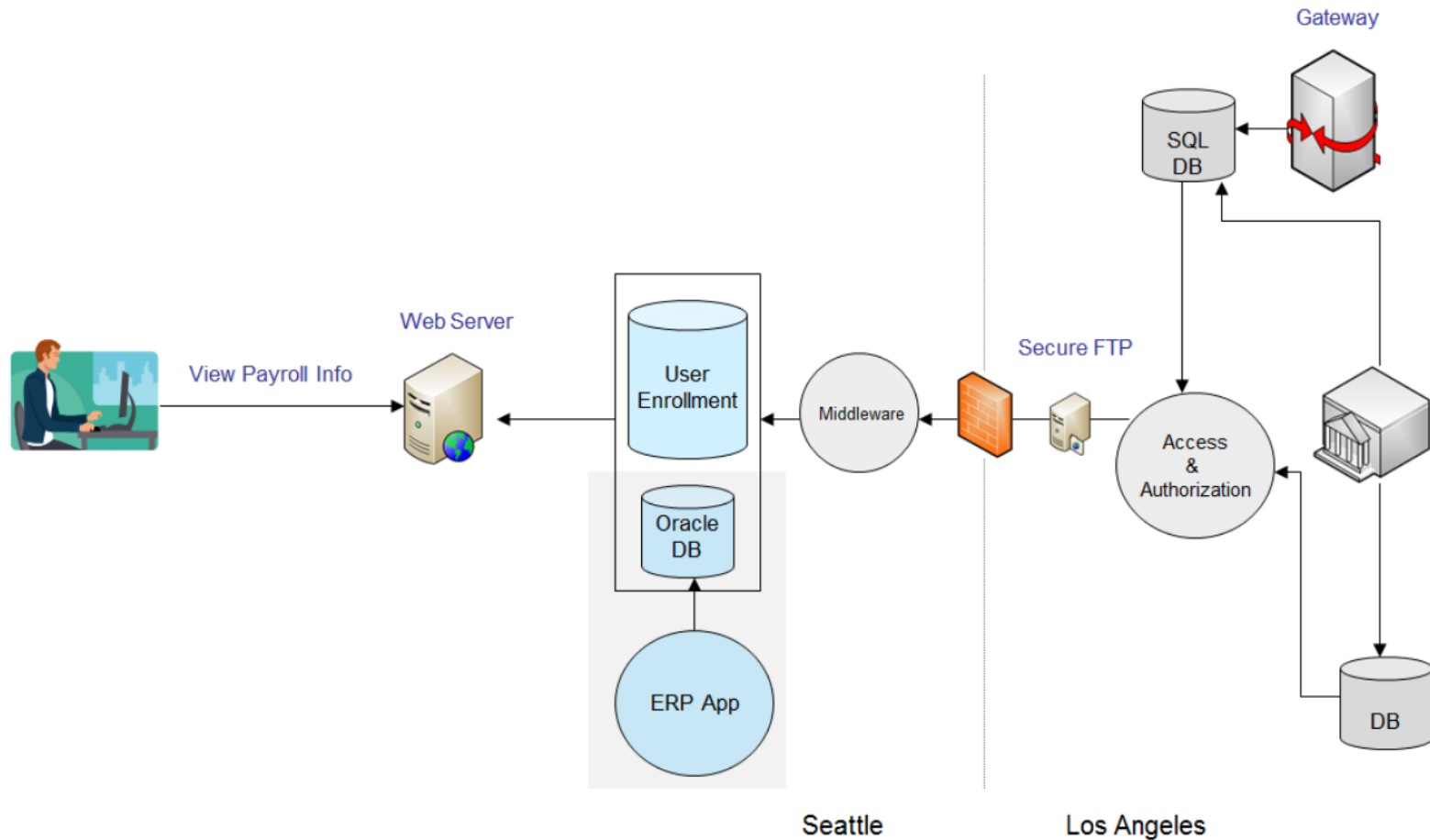
The table below lists the Ports, Protocols, and Services enabled in this information system. TCP ports are indicated with a T and UDP ports are indicated with a U.

Instruction: In the column labeled "Used By" please indicate the components of the information system that make use of the ports, protocols, and services. In the column labeled "Purpose" indicate the purpose for the service (e.g. system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing Provisional Authorization. Add more rows as needed.

Table 10-4. Ports, Protocols, and Services

Ports (T or U)	Protocols	Services	Purpose	Used By

Data Flow Diagram





Describing Security Controls in the SSP

- Security Control and enhancement requirement.
- Security control and enhancements require security control summary information.
- NOTE: The “-1” controls (e.g. AC-1, SC-1 etc.) describe Policies and Procedures.
- Some have multiple parameters and additional FedRAMP requirements
- All requirements (Part a – Part e) must have a response concerning implementations for the control.

Control Summary Definition

Responsible Role: the CSP should indicate what staff role within their organization is responsible for maintaining and implementing that particular security control. Examples of the types of role names may differ from CSP to CSP but could include role names such as:

- System Administrator
- Database Administrator
- Network Operations Analyst
- Network Engineer
- Configuration Management Team Lead
- IT Director
- Firewall Engineer

13.7.2 User Identification and Authentication (IA-2)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

IA-2	Control Summary Information
Responsible Role:	
Parameter:	
Implementation Status (check all that apply): <input type="checkbox"/> Implemented <input type="checkbox"/> Partially implemented <input type="checkbox"/> Planned <input type="checkbox"/> Alternative implementation <input type="checkbox"/> Not applicable	
Control Origination (check all that apply): <input type="checkbox"/> Service Provider Corporate <input type="checkbox"/> Service Provider System Specific <input type="checkbox"/> Service Provider Hybrid (Corporate and System Specific) <input type="checkbox"/> Configured by Customer (Customer System Specific) <input type="checkbox"/> Provided by Customer (Customer System Specific) <input type="checkbox"/> Shared (Service Provider and Customer Responsibility) <input type="checkbox"/> Inherited from pre-existing Provisional Authorization (PA) for <Information System Name>, <Date of PA>	
IA-2 What is the solution and how is it implemented?	



Control Origination Definitions

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from the CSP corporate network.	DNS from the corporate network provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular system at the CSP and the control is not part of the standard corporate controls.	A unique host based intrusion detection system (HIDS) is available on the service offering platform but is not available on the corporate network.
Service Provider Hybrid	A control that makes use of both corporate controls and additional controls that are specific to a particular system at the CSP.	There are scans of the corporate network infrastructure; scans of databases and web based application are system specific.
Configured by Customer	A control where the customer needs to apply a configuration in order to meet the control requirement.	User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http or https, etc), entering an IP range specific to their organization are configurable by the customer.
Provided by Customer	A control where the customer needs to provide additional hardware or software in order to meet the control requirement.	The customer provides a SAML SSO solution to implement two-factor authentication.
Shared	A control that is managed and implemented partially by the CSP and partially by the customer.	Security awareness training must be conducted by both the CSP and the customer.



Quick Tips: Easy Mistakes to Avoid

- Submitting an SSP without a Hardware or Software Inventory
- Incorrect references to supporting documents or guidelines
- Presenting non-applicable controls as implemented
- Not reviewing information pulled from other documents or sources
- Single sentence responses without details



Modifying the SSP

- You can modify the SSP to make it easier to describe your system
 - Add new sections
 - Do not remove required sections
- Make sure to provide sensitivity markings on the cover page and footer
 - Change to match company designation
 - Place markings in other sections as needed



User Guide

Describes how leveraging agencies use the system

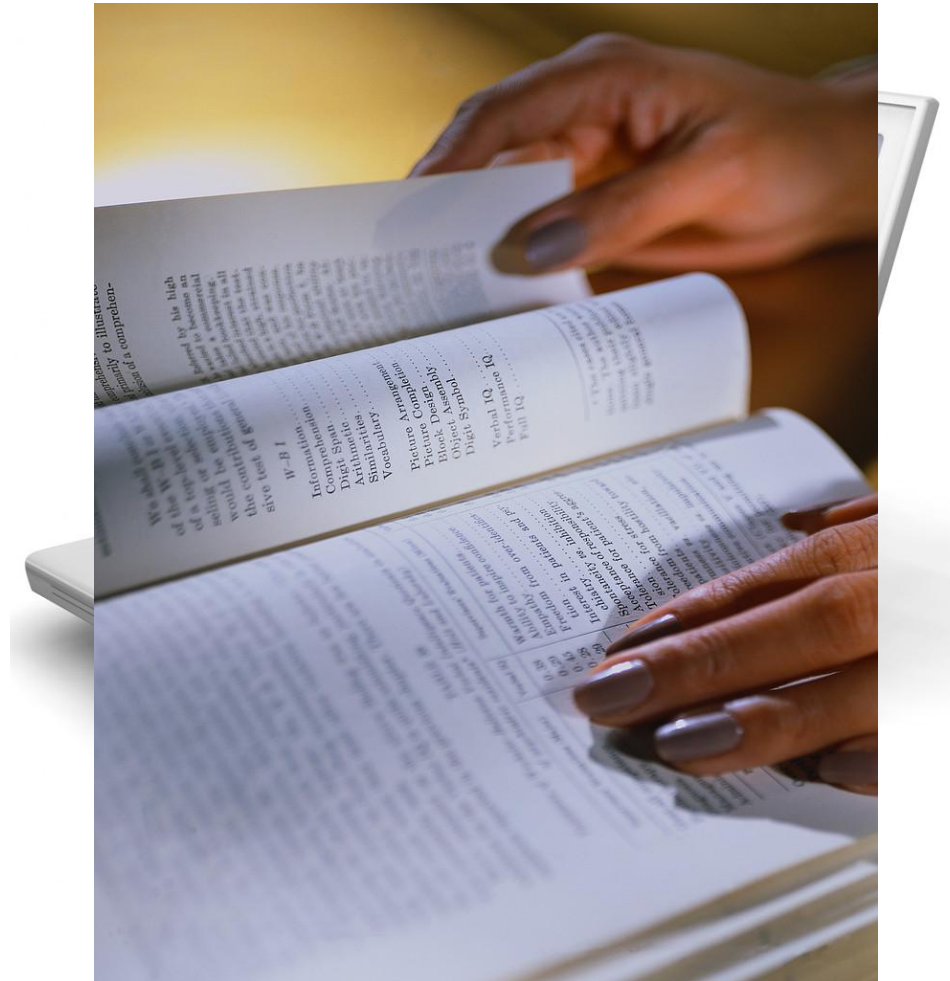




Supporting Documentation

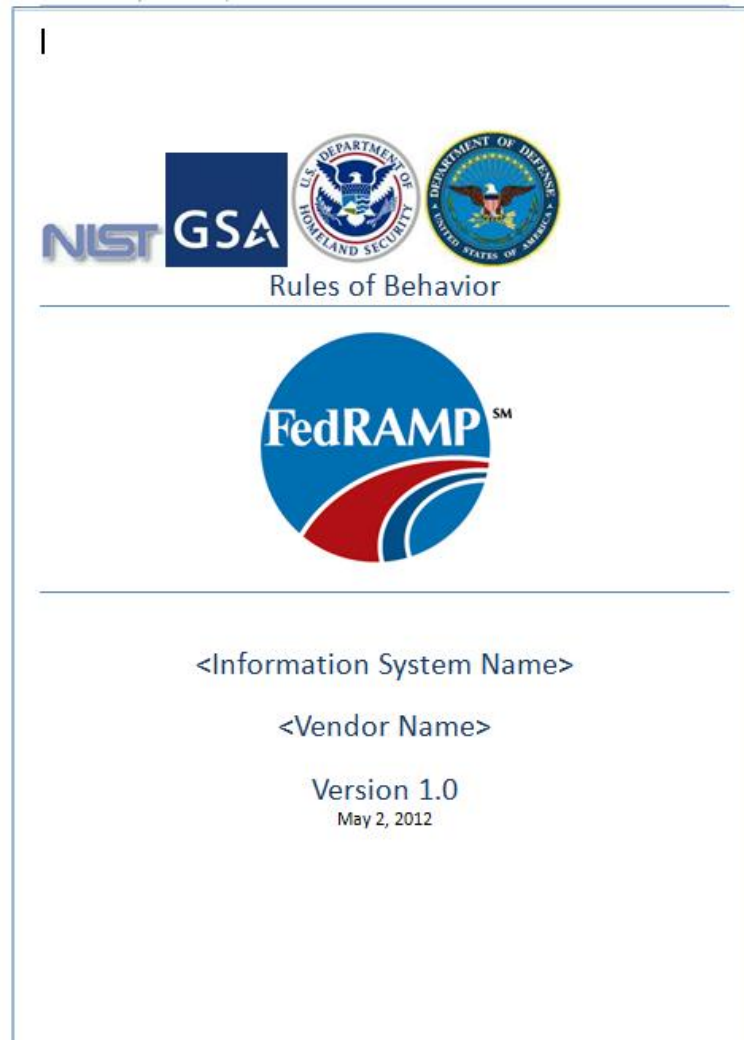
User Guide

Describes how leveraging agencies use the system



Rules of Behavior

Defines the rules that describe the system user's responsibilities and expected behavior with regard to information and information system usage and access.





Supporting Documentation

IT Contingency Plan

This document is used to define and test interim measures to recover information system services after a disruption. The ability to prove that system data can be routinely backed up and restored within agency specified parameters is necessary to limit the effects of any disaster and the subsequent recovery efforts.



<Vendor>

<Information System Name>

Version 1.0

May 2, 2012

Proprietary and Confidential
For Authorized Use Only

Configuration Management Plan

This plan describes how changes to the system are managed and tracked. The Configuration Management Plan should be consistent with NIST SP 800-128



Incident Response Plan

This plan documents how incidents are detected, reported, and escalated and should include timeframes, points of contact, and how incidents are handled and remediated. The Incident Response Plan should be consistent with NIST Special Publication 800-61.





Supporting Documentation


Privacy Threshold Analysis

This questionnaire is used to help determine if a Privacy Impact Assessment is required.

Privacy Impact Assessment

This document assesses what Personally Identifiable Information (PII) is captured and if it is being properly safeguarded. This deliverable is not always necessary.

Privacy Threshold Analysis
and Privacy Impact Assessment







<Vendor Name>

<Information System Name>

Version 1.0
May 2, 2012

Company Sensitive and Proprietary
For Authorized Use Only





What Makes a Good SSP

Key Areas of Focus for Documentation

- Completeness
- Compliant with FedRAMP policy and consistency with other package documents
- Delivery of supporting documentation
- Documentation is adequately referenced – e.g. : Policy, SOPs, Rules of Behavior, common control catalogs, waivers, exceptions, etc.

Content should address four (4) criteria :

- 1. What**
- 2. Who**
- 3. When**
- 4. How**

Proper level of detail for responses should be:

- Unambiguous
- Specific
- Complete
- Comprehensive
- Make sure the response is sufficient in length to properly answer the question



How to Document References

References To Other Documents Must:

- Be relevant to the control requirement
 - Be up to date...not from 4 years ago
 - Refer to a real document, not something that doesn't exist
-
- References Must Include:
 - Full document title
 - Publication date
 - Version number

Security settings of information technology products used with the XX system are set to the most restrictive mode consistent with information system operational requirements. From NIST Special Publication 800-70, guidance was received on necessary configuration settings for information technology products.



CM-6: Good Response

- A. All servers, databases, and workstations are configured according to the Center for Internet Security (Level 1) guidelines.
- B. Configuration settings are implemented and updated weekly by the System Administrator.
- C. No system component is exempt from compliance with CIS Level 1 settings
- D. Team X monitors and controls changes to configuration settings by using ZZZ monitoring system. Any and all changes must go through the official change request process.

More information may be found in the Configuration Management Plan.

- (1) CSP XYZ uses COTS Product AutoBlitz, Version 1.3 to manage, apply, and verify configuration settings. The nightly AutoBlitz report identifies and detects configuration changes made in the last 24 hours, including authorized and unauthorized changes
- (3) Upon detection of an unauthorized change or setting, a notice is automatically sent to the CSP XYZ SOC to report and track the incident.



Resources: Guide to Understanding FedRAMP



The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Are you a...?

Federal Agency



What can FedRAMP do for your agency?

CSP Cloud Service Provider



Get a FedRAMP security authorization.

3PAO Third Party Assessors



Become a FedRAMP accredited assessor.

FEDRAMP HAS NOW LAUNCHED

To apply or sponsor a system for authorization, please fill out the FedRAMP application [here](#).

CONTACTS

General Inquiries
info@fedramp.gov

Press Inquiries
202-501-9113

KEY LINKS

[FedRAMP Initiation Request](#)

[Accredited 3PAOs](#)

[Authorized CSPs](#)

KEY DOCUMENTS

[FedRAMP Concept of Operations \(CONOPS\)](#)

[FedRAMP Security Controls](#)

[FedRAMP Templates](#)

[FedRAMP Continuous Monitoring Strategy Guide](#)

[FedRAMP Standard Contract Clauses](#)

[FedRAMP Control-Specific Contract Clauses](#)

[Guide to Understanding FedRAMP](#)

[FedRAMP Policy Memo \(OMB\)](#)

[3PAO Program Description](#)

[FedRAMP JAB Charter](#)

Guide to Understanding FedRAMP





In Summary...

- Three main parts of the SSP
- Avoid easy mistakes by paying attention to details
- Structure your response
 - Who, What, When, How
 - Be consistent throughout the document
 - Provide the right details in your answer
- Read the Guide to Understanding FedRAMP
 - Review the Prep Checklist



Question and Answer Session

For more information, please contact us or visit us at any of the following websites:

<http://FedRAMP.gov>

<http://gsa.gov/FedRAMP>

Email: info@fedramp.gov

Follow us on [twitter](#) @ FederalCloud





For more information, please contact us or visit us at any of the following websites:

<http://FedRAMP.gov>

<http://gsa.gov/FedRAMP>

Email: info@fedramp.gov

Follow us on [twitter](#) @ FederalCloud