TEVORA™

Addendum A

Composing a FedRAMP System Security Plan

Kevin Liang
Taiba Zadran
with guidance and revisions from
Kaitlyn Bestenheider
Troy Dahlin

July 15, 2020

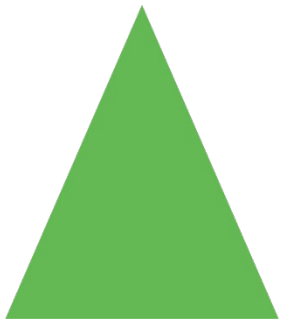

Table of Contents

System Security Plan Overview

A System Security Plan (SSP) is the comprehensive document that provides an overview of an organization's system security requirements. The SSP details the system architecture, security controls, and the responsibilities of individuals who have access to the system. This document allows personnel to record and review the current conditions and plans to secure the system. The purpose of the SSP is to provide priority to information security by outlining the security status and plans to protect organizational assets. This includes the prevention of unauthorized access, disruption of services, and unauthorized modification of systems or services.

The SSP also provides narrative and reference to individuals seeking information about the system's security. Some of the main components of an SSP include security control implementations, system components, service inventory, depictions of system data flows, and boundaries. The main components depict a complete guide to provide all the information needed to further enhance information security objectives. Furthermore, a Federal Risk and Authorization Management Program (FedRAMP) SSP will include additional controls above the NIST baseline that specifically address cloud security risks.

An established proficiency and knowledge of an SSP is strongly recommended before continuing with the development of an SSP.

Preparing to Write an SSP

An SSP is an extensive document that requires considerable time and resource commitment to complete. Before beginning to document an SSP, it may be necessary to onboard advisors, including technical consultants and technical subject matter experts (SME). These SMEs can offer guidance to address the risks of organizational operations with or without an SSP. This allows administrators and management to make an informed decision regarding the benefits of a developing an SSP for the organization.

Once the decision to development an SSP is made, some organizations may elect to bring in an independent, third-party consultant to assist in the documentation and review of all relevant security controls. The consultant(s) should offer expertise on the technical subjects including knowledge of system network architecture, technical roles and responsibilities, and implementation of security controls.

Once an organization identifies all necessary responsible parties and allocates the documentation responsibilities, the organization can begin composing the SSP. Organizations may find it beneficial to appoint one or more technical writers to lead the composition of control implementation to develop a coherent SSP. The writers can use information and templates available on the FedRAMP website (see Appendix: References below). This will provide a starting point in the development phase. When using a pre-crafted template, writers can input the necessary control information into the template.

The following will outline the main sections found in a standard SSP using the template provided by FedRAMP.

Key SSP Sections and Concepts

The following section will list key sections of an SSP and their respective descriptions, as well as the necessary attachments required for a successful SSP. An SSP that uses the FedRAMP template includes 15 sections and 13 additional attachments:

1. Information System Name/Title
2. Information System Categorization
3. Information System Owner
4. Authorizing Official
5. Other Designated Contacts
6. Assignment of Security Responsibility
7. Information System Operational Status
8. Information System Type
9. General System Description
10. System Environment and Inventory
11. System Interconnections
12. Laws, Regulations, Standards and Guidance
13. Minimum Security Controls
    - Access Control (AC)
    - Awareness and Training (AT)
    - Audit and Accountability (AU)
    - Security Assessment and Authorization (CA)
    - Configuration Management (CM)
    - Contingency Planning (CP)
    - Identification and Authentication (IA)
    - Incident Response (IR)
    - Maintenance (MA)
    - Media Protection (MP)
    - Physical and Environmental Protection (PW)
    - Planning (PL)
    - Personnel Security (PS)
    - Risk Assessment (RA)
    - System and Services Acquisition (SA)
    - System and Communications Protection (SC)
    - System and Information Integrity (SI)
14. Acronyms
15. Attachments
    - Attachment 1: Information Security Policies and Procedures
    - Attachment 2: User Guide
    - Attachment 3: Digital Identity Worksheet
    - Attachment 4: Privacy Threshold Analysis / Privacy Impact Assessment
    - Attachment 5: Rules of Behavior
    - Attachment 6: Information System Contingency Plan
    - Attachment 7: Configuration Management Plan
    - Attachment 8: Incident Response Plan
    - Attachment 9: Control Implementation Summary Workbook
    - Attachment 10: FIPS 199

- Attachment 11: Separation of Duties Matrix
- Attachment 12: FedRAMP Laws and Regulations
- Attachment 13: FedRAMP Inventory Workbook

For more information on each of these sections and a description of the critical information needed, see Attachment A – Composing an SSP.

The introduction to the SSP must describe specific information about a system including System Categorization, Authorization Boundary, and scope. It is critical to define the scope of the SSP accurately to prevent unauthorized information from entering or exiting the Authorization Boundary.

Information System Name/Title

To begin, the Cloud Service Provider (CSP) must identify the name of the system and any short names that may be used in the SSP. This will also include the FedRAMP application number as a unique identifier. The unique identifier can be used to search in the FedRAMP database, allowing users to locate and collect system information and security metrics.

Information System Categorization

The system categorization is used to describe the depth of the SSP. Since this will also determine which controls are addressed within the SSP, it is a critical first step in the process of documenting an SSP. The system categorization uses the FIPS 199: Standards for Security Categorization of Federal Information and Information Systems (FIPS 199) to choose between Low, Moderate, or High system sensitivity levels. FIPS-199 is used to classify the entire information system based on the types of information that may be stored within the information system.

Information Types

This framework uses the NIST Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories (NIST 800-60) to delineate the differences between information types. Both FIPS 199 and NIST SP 800-60 uses the confidentiality, integrity, and availability (CIA) triad model to classify information types. Each part of the CIA triad is also included in the system, determining potential impact of Low, Moderate, High.

- Low indicates that the risk of impact has limited effect on the organization.
- Moderate indicates that the risk of impact has serious effect on the organization.
- High indicates that the risk of impact has catastrophic effect on the organization.

FIPS-199 is used to classify the entire information system. NIST 800-60 is used to classify individual data types within an information system. The information is categorized with a high watermark to classify the entire system. For example, an information system can have almost entirely Low information types, but a single High classification under one of the CIA triad categories can result in the entire system being classified as a High baseline.

Security Objectives Categorization

The security objectives categorization produces a summary of the CIA triad. It follows the high-water mark method which uses the highest sensitivity level of the CIA triad as its baseline security categorization. Any security controls and standards implemented to the system would follow that baseline categorization.

As an example, consider an information system containing personally identifiable information (PII). The confidentiality is marked as High, integrity is marked as Moderate, and availability is marked at Low. The high-water mark decision would follow the greatest potential impact, which is the High confidentiality mark. As a

result, the whole PII system would have a “High” system security categorization.

Digital Identity Determination

Digital Identity as outlined in NIST Special Publication 800-63: Digital Identity Guidelines (NIST 800-63) defines three categories for a system to identify users with their digital counterparts. Digital identity includes any user’s alias used over networks to distinguish oneself. Each category also includes three possible levels where the higher the level, the more assurance is required to verify users. The purpose is to encapsulate the confidence that the user identity is needed to determine legitimate authorization. The three categories are:

- Identity Assurance Level (IAL) is the identity proofing process to describe the methods to vet a person’s digital identity against their real-life identity.
- Authenticator Assurance Level (AAL) is the authentication process to describe the methods used to verify legitimate access to a system.
- Federation Assurance Level (FAL) is the assertion in a federated environment to describe the methods to verify identities across different identity domains. The identity domains do not share the same credentials as another domain. This requires the user to be verified each time when accessing a new session.

Each level increases the sensitivity of the information on the system. For example, AAL1 requires single-factor authentication, while AAL3 requires multi-factor authentication using approved cryptographic techniques.

Significant Roles

An SSP must identify individuals who are assigned significant roles in the system. The identification of roles helps readers determine individuals who manage the system and are points of contact for inquiring about system access and changes. The roles include:

Information System Owner

The Information System Owner (SO) is the primary individual who is the functional proponent for the information system. The SO is responsible for any procurements, developments, and operations of the information system. The SO is an individual who could be the sole manager of the system and must be notified of any incidents or changes that occur on the system.

Authorizing Official

The Authorizing Official (AO) is the primary individual who assumes responsibility for decisions on the acceptable level of risk on the system including operations, assets, and other individuals. The AO is responsible for choosing which system activities are acceptable by assessing how much exposed risk could occur if conducted.

In addition, due to the nature of the SSP and its objective to outline the system specific to security, the following are individuals with security roles and responsibilities.

Information System Security Officer

The Information System Security Officer (ISSO) is the principal advisor for information and implementation of controls involving the security of the system. The ISSO is responsible for protecting the organization's network infrastructure and information to improve security measures against malicious attacks and unauthorized access to decrease risk in business disruption, confidential data loss, and financial loss.

The AO, as mentioned previously, also takes part in security decision making as it relates to the system.

Other Designated Contacts

- Information System Management Point of Contact: the individual who oversees operations and individuals. They can identify personnel whom they have delegated roles to within the system.
- Information System Security Point of Contact: the individual who oversees the security activities. They can identify individuals with regards to privileged access and operations that can affect security risks to the system.
- Information System Technical Point of Contact: the individual who offers advice on specific operations, based on technical specialization.
- While not specified in the standard FedRAMP SSP template, Tevora recommends organizations include the Information System Legal Counsel Point of Contact. This is an individual who provides legal advice according to system related laws and regulations. Additionally, this individual can represent the organization in a legal matter.

Please note, an SSP can identify additional key points of contact as necessary to document the individuals responsible for the information system.

Information System Operation Status

The SSP includes the operational status, which outlines the condition of the system. This describes what stage of production or development that the system is in and can include operational, under development, major modification, and other. More than one status can be selected at a time and should be updated before publishing the final version.

- Operational: The system is operating and in production.
- Under Development: The system is being designed, developed, or implemented.
- Major Modification: The system is undergoing a major change, development, or transition.
- Other: This status is an opportunity for the individual managing the SSP to detail other possible statuses of the system.

Information System Type

An SSP includes the information system type which identifies that the system will be limited to categorization by cloud systems strictly related to FedRAMP. The following specifies the purpose of the system as it relates to the cloud.

Cloud Service Models

The Cloud Service Models section outlines the architecture layers, categorizing the system by its purpose and services. The SSP describes four cloud architecture layers a system can use. The layers include the following:

- Software as a Service (SaaS) where software can directly interact with end users to deliver services.
- Platform as a Service (PaaS) where services such as OS and applications can be used for development and deployment.
- Infrastructure as a Service (IaaS) where storage, server, and network services can be used to host hardware, network, and servers.
- Other includes any other layer that does not reside in the cloud but is considered interconnected to the system. This can include the physical layers that is within the scope of the system.

Cloud Deployment Model

The cloud deployment model describes the infrastructure of the system that is represented by what entities can access it. It identifies the intended users the cloud will provide services for and outlines the purpose of the system. The four deployments models include:

- Public is accessible by public users.
- Private is accessible by only designated organizations.
- Government Only Community is accessible by only federal agencies.
- Hybrid is accessible by both public users and designated organizations.

Leveraged Authorizations

The leveraged authorizations describe pre-existing FedRAMP authorized cloud services that will be used in combination with the current system. The purpose of leveraged authorizations is to help achieve a sufficient level of operations of the system.

General System Description

The general system description further defines the scope of the system by explicitly identifying the purpose, individuals, and architecture of the system.

System Function or Purpose

The system function or purpose section specifically defines the objective of the system. For example, the website it will be supporting, functions users will have access to, and how the system will play a role in the operations of the organization.

Information System Components and Boundaries

The Information System Components and Boundaries section defines the specific boundaries and the components that would monitor and control those boundaries. This section should include diagrams outlining the system to illustrate authorization boundaries, as well as logical and physical topologies.

Types of Users

This section defines the types of users and the level of privilege they have to the system. The users specified are individuals who could expose a level of risk as defined in NIST Special Publication 800-53 Revision 4: Recommended Security Controls for Federal Information Systems and Organizations (NIST 800-53 Rev. 4). Some of the roles include administrative, managerial, and development responsibilities.

The following identifies individuals who are potential insider threats or external threats.

- Internal users are employees or contractors hired by the service provider. They are defined as users with specific roles to support the system as intended by the service provider.
- External users are all other individuals that are not internal users.

The purpose of the roles is to identify individuals with elevated access and document their potential risk to the system.

- Privileged (P) users have administrative access. They have user privileges that could access, modify, or delete system assets. They are considered a high risk to the organization.
- Non-Privileged (NP) users are ordinary users that do not have access to administrative roles, however, NP users have limited access to the system, allowing minimal activity and functionality within the system.
- No Logical Access (NLA) users are individuals who do not have access to the system. They hold no approved functions within the system and therefore do not have permission to conduct activity within it.

The roles must also be identified with their sensitivity level. The sensitivity level categorizes the amount of risk the individual poses from their responsibilities and further encapsulates the level of impact the individual can cause in combination with their privileges.

- Limited sensitivity level indicates the individual's potential negative impact to the organization can have marginal effects.
- Moderate sensitivity level indicates the individual's potential negative impact to the organization can have serious effects.
- High sensitivity level indicates the individual's potential negative impact to the organization can have catastrophic effects.

The roles must also identify the users' authorized privileges, which are system services and functions they can access. This helps identify the possible authorized tasks the individual is permitted to perform and to determine the level of risk the individual can cause. Any activity outside of these authorized tasks can most likely be considered illegitimate.

The roles must also identify the functions performed, which is further elaborated on in the Authorized Privileges section.

Network Architecture

The Network Architecture section is similar to the Components and Boundaries section of the SSP with more specific illustrations to outline the network. The network architecture should be defined through a logical network topology where all network components are displayed.

System Environment and Inventory

Data Flow

The Data-Flow Diagram outlines the flow of mainly confidential information, how it is handled, and its boundaries. The diagram illustrates the points in the system where information is in transition or at rest. The diagram should outline the route and process of the information starting from the end-user to the information storage. To emphasize the process, data-flow diagrams should include actions done by each system.

Ports, Protocols, and Services

This section displays all the active ports with their protocols and services.

- Ports are communication endpoints in computer networking and help different networks communicate with each other in a consensus where hosts, protocols, and services are agreed upon when sending information packets.
- Protocols complete port network communications by defining the specific rules on how each exchange in their messaging is formatted. This includes rules, syntax of how the language of the message is written, and the services that are provided.
- Services outline the utility of applications on the network. They provide the functions of the ports and protocols, including data storage, data manipulation, and communication.

This section should be followed by the business justification of why the port is active and what systems would be used by the port. To follow best practices in cybersecurity, each port must serve a legitimate purpose for operations to decrease the number of vulnerabilities points that attackers can exploit. By including the systems and individuals that use the port, it would narrow down the number of users that have legitimate access to them, preventing unnecessary usage of ports which may expose the system to potential vulnerabilities.

System Interconnections

The system interconnection section lists the external networks the system is connected to. The external networks are included in the authorization boundary, but have a connection to access, process, and transmit data to and from the authorization boundary.

The system interconnections should also include information about the connections to external systems. By providing detail about the network, readers can determine the level of risk the network poses to the SSP system. Some details include the following:

- Service Processor IP Address and Interface is the network name through computer networking terms to distinguish its network domain. This can include the website URL or the IP address from its interface identifier.
- External Organization Name and IP Address of System is the organizational name used to identify which organization and domain the external system belongs within.
- Connection Security describes the security measures in place to establish confidence of authorizing the connection from the SSP to the external system. Some secure connection methods include SSH and SSL/TLS.
- Data Direction indicates which direction the data is flowing. The data direction also identifies the risks and potential impact the external network can have on the SSP system. With incoming data flow, the risks include the potential installation of malware which can disrupt the organization's operations. With outgoing data flow, the risks include the potential of insider threat where individuals export confidential information from the system.
- Information Being Transmitted identifies the type of information that is authorized for transit. This includes the specific organizational data, traffic, and confidential information.
- Port or Circuit Numbers identifies the specific port that the external network has access to for communication with the SSP system.

Laws, Regulations, Standards, and Guidance

The Laws, Regulations, Standards, and Guidance section outlines the relevant legislations and standards that apply to the system. It contains the scope of the SSP within the specific laws, standards, and references. Additional information on FedRAMP laws, regulations, standards, and guidance can be found in the "FedRAMP Laws and Regulations Template" in the References section below.

Applicable Laws and Regulations

The inclusion of Applicable Laws and Regulations section addresses the legislation imposed on the system to avoid legislative repercussions that apply to certain organizations.

Applicable Standards and Guidance

The inclusion of the Applicable Standards and Guidance section addresses the references needed to establish the standard that was used to develop the SSP. The purpose of this section is to define the methods and standards used by the SSP writer to verify the SSP development was done relevant to current security standards.

Controls Documentation

The Controls Documentation section purpose is to outline each control by its requirements, implementation status, and the solutions provided to the organization. It verifies the progress of the security control while illustrating why the implementation is necessary.

General Controls Assignment Parameters

The General Controls Assignment Parameter section addresses the differences in acceptable risk from each organization, by including variables in the SSP that the developers can adjust according to each control. This maximizes the effects of the security controls according to the organization's requirements while preventing unnecessary implementation of the security-based standards, instead implementing based on individual organizational needs. Examples of control assignment parameters include the following:

- Assignment: organization-defined information system account types defines the specific account types in the system that the control would affect.
- Assignment: organization-defined personnel or roles defines the specific individuals in the system that the control would need to involve fulfilling the control implementation.
- Assignment: organization-defined procedures or conditions defines the specific procedural documentation that the control would adhere to fully accomplish the control implementation.
- Assignment: organization-defined frequency defines the specific rate needed to conduct that activity for the control to fully accomplish the control implementation.

Control Summary Information

- Implementation Status indicates the current condition of implementing a security control to the system.
    - Implemented states that the security control is fully and correctly implemented.
    - Partially Implemented states that only part of the security control is implemented.
    - Planned sates that the security control implementation is currently ongoing.
    - Alternative implementation states that the system has already implemented a different security control that fulfills the purpose of the intended control.
    - Not applicable states that the security control, if implemented or not, does not affect the system.
- Control Origination indicates the types of participants that are required to implement the control.
    - Service Provider Corporate: A control that originates from the CSP corporate network. Service Provider System Specific: A control specific to a system at the CSP and the control is not part of the service provider corporate controls.
    - Service Provider Hybrid: A control that makes use of both corporate controls and additional controls specific to a system at the CSP.
    - Configured by Customer (Customer System Specific): A control where the customer needs to apply a configuration to meet the control requirement.
    - Provided by Customer (Customer System Specific): A control where the customer needs to provide additional hardware or software to meet the control requirement.
    - Shared (Service Provider and Customer Responsibility): A control that is managed and implemented partially by the CSP and partially by the customer.
    - Inherited from pre-existing FedRAMP Authorization: A control that is inherited from another CSP system that has already received an Authorization.

What is the solution and how is it implemented?

This section describes the specific security controls by outlining its relevancy and explaining how the control is applied to the system. To accomplish this, the section should reference any relevant policy or procedural documentation and outline the relevant individuals' functions and privileges to perform appropriate tasks within the control's restrictions.

The section should also include the affected systems and their functions to describe any changes to the system once the control is implemented.
For each control, the technical writer will document how the control is met as if there is no other documentation for this control. It will be down to each lettered line item of the control, but any sub-requirements beyond that must also be described in the relevant spaces.

Attachments

The FedRAMP SSP includes 13 relevant attachments. Each attachment may require multiple documents to be compressed to a single file for presentation to the Joint Authorization Board (JAB). Below is additional information and resources for each SSP attachment.

ATTACHMENT 1: Information Security Policies and Procedures

Attachment 1 may be fulfilled by documents that encompass information security which will be reviewed for quality. These documents may be security standards, policies, and procedures for system architecture. The standards, policies, and procedures could be derived from the following security controls from NIST 800-53:

- AC – Access Control
- AU – Audit and Accountability
- AT – Awareness and Training
- CM – Configuration Management
- CP – Contingency Planning
- IA – Identification and Authentication
- IR – Incident Response
- MA – Maintenance
- MP – Media Protection
- PS – Personnel Security
- PE – Physical and Environmental Protection
- PL – Planning
- PM – Program Management
- RA – Risk Assessment
- CA – Security Assessment and Authorization
- SC – System and Communications Protection
- SI – System and Information Integrity
- SA – System and Services Acquisition

ATTACHMENT 2: User Guide

Authorization Packages must include a User Guide attachment, which will be reviewed for quality. They are documents for users to follow which will guide them through system and organizational processes. The documents instruct the user on their responsibilities and how to appropriately use the system. For example, if a user must provision users, it should explain how to do so. If a user must maintain a system in a certain capacity, the user guide should provide instruction and direction on how to do so.

ATTACHMENT 3: Digital Identity Worksheet

A template for this document, Digital Identity Requirements, can be found on the FedRAMP website (see "Document Repository" in the References section below). It has been developed to provide guidance on Digital Identity requirements in support of achieving and maintaining security authorization that meets FedRAMP requirements. FedRAMP follows the NIST guidance and this document shows how FedRAMP implements it. As stated in FedRAMP Authorization Guide: 2020 Internship Whitepaper:

> "Digital Identity as outlined in NIST Special Publication 800-63: Digital Identity Guidelines (NIST 800-63) defines it as three categories for a system to identify users with their digital counterparts. Digital identity includes any user's alias used over networks to distinguish oneself. Each category also includes three possible levels where the higher the level, the more assurance is required to verifying users. The purpose is to encapsulate the confidence that the identity of the user accessing the system is needed determine legitimate authorization."

ATTACHMENT 4: Privacy Impact Assessment Template

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and a Privacy Impact Assessment (PIA) if necessary, which will be reviewed for quality. The PTA and PIA templates include a summary of laws, regulations, and guidance related to privacy issues in Attachment 12 - FedRAMP Laws and Regulations. An organization may need to perform a PIA if they handle Personal Identifiable Information (PII). A PTA may need to be completed beforehand to determine if the organization handles PII.

ATTACHMENT 5: Rules of Behavior Template

All Authorization Packages must include a Rules of Behavior (RoB) attachment, which will be reviewed for quality. The template provides two sets of examples for rules of behavior: Internal Users and External Users. An organization should implement and modify each set of behaviors appropriate to the security of the organization's system. The RoB controls are associated with user responsibilities and certain expectations of behavior for following security procedures, policies, and standards.

ATTACHMENT 6: Information System Contingency Plan Template

All Authorization Packages must include an Information System Contingency Plan (ISCP) which will be reviewed for quality. A template for Information System Contingency Plan can be found on the FedRAMP website (see "Template Repository" in the References section below). An ISCP denotes interim measures to recover information system services following an unprecedented emergency or system disruption. These disruptions may be natural disasters, outages, loss of equipment, or other damages that result in a loss. The system contingency plan delivers an approach to ensure system recovery and minimized disruption time. The CSP establishes multiple roles and responsibilities for responding to outages, disasters, or disruptions. The

main personnel who is selected is the Contingency Planning Director (CPD), who owns the responsibility for all facets of contingency and disaster recovery planning and execution.

ATTACHMENT 7: Configuration Management Plan

All Authorization Packages must include a Configuration Management Plan (CMP) which will be reviewed for quality. Configuration management is the ongoing process of identifying and managing changes to deliverables and other products. The purpose of this plan is to define, document, control, implement, and audit changes to products. Those products may be software (applications or code), hardware (routers, switches, servers), or networks.

ATTACHMENT 8: Incident Response Plan

All Authorization packages must include an Incident Response Plan procedure as part of the SSP package. This procedure ultimately delivers a process to recover from an incident that has occurred within the organization. It should at least address the following: scope, roles and responsibilities, security incident types, security incident categories, security incident severity, security incident reporting, and security incident management lifecycle.
An Incident Response Plan should also carry out the following processes: preparation, detection and analysis, containment, eradication, recovery, and lessons learned of the incident. More information on Incident Response can be found on NIST 800-53 website (and on “NIST: Incident Response” in the References section below).

ATTACHMENT 9: Control Implementation Summary

All Authorization Packages must include a Control Implementation Summary (CIS) to be submitted with the SSP as part of the final security package, which will be reviewed for quality. A template for Control Implementation Summary can be found on the FedRAMP website (see “Templates” in the References section below). The CIS delineates the control responsibilities of CSPs and Federal Agencies and provides a summary of all required controls and enhancements across the system.

ATTACHMENT 10: Federal Information Processing Standard-199 Categorization Template

All Authorization packages must include the Federal Information Processing Standard-199 (FIPS-199) as part of the SSP package. FIPS-199 creates security categories of information systems that are used by the Federal Government. It also establishes a common security framework and an understanding of security that the federal government can provide effective management on and oversight of information systems. The standards apply to all agencies that deal with government information, being state, local, and tribal governments as well as private sector organizations.

ATTACHMENT 11: Separation of Duties Matrix

The purpose of this document is to provide separation of duties to personnel within an organization to avoid the potential abuse of unauthorized privileges to the system. Role or rule-based access to objects, files or applications can be implemented to increase information security. For example, dividing mission functions and

information system support functions among different individuals or roles. This also includes conducting information system support functions with different individuals and ensuring that personnel administering access control functions do not also administer audit functions.

ATTACHMENT 12: FedRAMP Laws and Regulations

All Authorization Packages must include a FedRAMP Laws and Regulations attachment, which will be reviewed for quality. A template for FedRAMP Laws and Regulations can be found on the FedRAMP website (see “Templates” in the References section below). This template provides a single source for applicable FedRAMP laws, regulations, standards, and guidance along with the documents: SSP, SAR, SAP, and other applicable documents.

ATTACHMENT 13: FedRAMP Integrated Inventory Workbook Template

The FedRAMP Integrated Inventory Workbook Template combines all the inventory information previously required in five FedRAMP templates that included the SSP, ISCP, SAP, SAR, and POA&M. The CSP should use this inventory template to portray inventory items for the entire operating system infrastructure, software, and databases as part of preparing phase for the readiness assessment and for the initial authorization of the system. The service offering is in the monitoring phase of its lifecycle, and the CSP should use this template to describe and submit inventory for the monthly continuous monitoring efforts. Each document should be “saved as” monthly to keep month-to-month submissions of the inventory.

Conclusion

The SSP provides precedence from its capacity to outline the security status and requirements. This ultimately emphasizes the importance of security on the system. The value of the SSP derives from personnel activity using it as reference to enforce security measures. This is crucial as security protects organizations’ important assets such as information, operations, IT systems, data, and technology to prevent potential loss of confidential data. If there is a request for information about the organizations system architecture, security controls, and significant individuals related to security in the system, the SSP is the key document they would review first. Ultimately, the SSP is the foundation for all system security deployed on the organization and contains all the information needed to review its security.

Appendix: Glossary

- **3PAO** – Third Party Assessment Organization
- **Agency** – Federal Agency that grants ATO to CSP for its CSO
- **AO** – Authorizing Official
- **Authorization Package** – Package containing evidence for Authorization including SSP, SAP, SAR, POA&M, Continuous Monitoring Plan, ATO Letter
- **CSO** – Cloud Service Offering
- **CSP** – Cloud Service Provider
- **FedRAMP** – Federal Risk and Authorization Management Program
- **FedRAMP Authorized** – Status granted by FedRAMP PMO that a CSO is compliant with FedRAMP.
- **FIPS** – Federal Information Processing Standards
- **FIPS 199** – Standards for Security Categorization of Federal Information and Information Systems
- **NIST** – National Institute Standards of Technology
- **ISSO** – Information System Security Officer
- **POA&M** – Plan of Actions and Milestones
- **PMO** – Program Management Office
- **RAR** – Readiness Assessment Plan
- **SAP** – Security Assessment Plan
- **SAR** – Security Assessment Report
- **SSP** – System Security Plan

Appendix: References

- FedRAMP Moderate Readiness Assessment Report (RAR) Template (August 2018) found on the FedRAMP website's Template Repository.
- FedRAMP System Security Plan (SSP) Moderate Baseline Template (August 2018) found on the FedRAMP website's Template Repository.
- FedRAMP Initial Authorization Package Checklist (March 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 3 - Digital Identity Document (February 2018) found on the FedRAMP website's Document Repository
- SSP ATTACHMENT 4 - FedRAMP Privacy Impact Assessment (PIA) Template (June 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 5 - FedRAMP Rules of Behavior (RoB) Template (June 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 6 - FedRAMP Information System Contingency Plan (ISCP) Template (June 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 9 - FedRAMP High Control Implementation Summary (CIS) Workbook Template (June 2017) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 12 - FedRAMP Laws and Regulations Template (Aug 2018) found on the FedRAMP website's Template Repository.
- SSP ATTACHMENT 13 - ATO Integrated Inventory Workbook Template (June 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Security Assessment Plan (SAP) Template (June 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Security Assessment Report (SAR) Template (June 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Plan of Action and Milestones (POA&M) Template (March 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Agency Authorization Review Report Sample Template (June 2019) found on the FedRAMP website's Template Repository.
- FedRAMP ATO Letter Template (June 2019) found on the FedRAMP website's Template Repository.
- FedRAMP Annual Security Assessment Plan (SAP) Template (June 2017) found on the FedRAMP website's Template Repository.
- FedRAMP Annual Security Assessment Report (SAR) Template (June 2017) found on the FedRAMP website's Template Repository.
- NIST Special Publication 800-53 (Rev. 4 January 2015) found on the NIST website's Computer Security Resource Center.
- NIST: Incident Response found on the website NIST 800-53 Special Publication .
- NIST Special Publication 800-60 (Rev. 1 June 2004) found on the NIST website's Computer Security Resource Center.
- FIPS PUB 199 (February 2004) found on the NIST website's Computer Security Resource Center.

For further guidance, review NIST SP 800-18 Rev. 1: Guide for Developing Security Plans for Federal Information Systems, which delves into greater detail of explicit system components, security controls, significant individuals, and risk assessments.

Kevin Liang, Federal Consultant Development Program

Primary Role	Kevin was part of the Consultant Development Program at Tevora and was responsible for providing supporting work during assessments and the report writing process.
Notable Accomplishments	Kevin developed multiple personal projects utilizing his established private virtual home lab containing resources and platforms to conduct tests and experiments. The experiments include White-hat hacking projects to breach into his personal network and another experiment is engaging in available cloud computing services. His objective is to obtain hands-on experience from subsequent research on modern cybersecurity topics.
Certification and Training	Kevin earned his Bachelor of Science in Information Technology from George Mason University and holds certificate to the NSA/DHA National CAE in Information Assurance and Cyber Defense. He also holds his CompTIA Security+ certification.
Tenure	Kevin was with Tevora from January 2020 until April 2020.

Taiba Zadran, Information Security Associate

Primary Role	Taiba is an Information Security Associate at Tevora and is responsible for providing supporting work during assessments and the report writing process.
Notable Accomplishments	Taiba was previously an intern at Tevora through the Consultant Development program. Before that, she interned at Symantec Corporation through the Year Up program in 2019.
Certification and Training	Taiba is currently attending George Mason University, pursuing a bachelor's degree in information technology and cyber security. She is currently part of AllCyber, a non-profit organization aiming to advance students' cyber security skills. Taiba also holds her CompTIA Security+ certification and has completed a CCNA Cyber Ops training program with Per Scholas and was a participant in the National Cyber League competition.
Tenure	Taiba has been with Tevora since January 2020.

Kaitlyn Bestenheider, Senior Information Security Analyst

Primary Role	Kaitlyn is an Information Security Analyst at Tevora and is responsible for providing supporting work during assessments and the report writing process.
Notable Accomplishments	Kaitlyn has served as a high school cybersecurity instructor at Rockland County BOCES Career and Technical School in Nyack, NY, where she helped second year students prepare for their CompTIA Security+. Kaitlyn has also worked as a Digital Marketing Specialist for Silver Tips Tea, where she provided in-house technical support, developed a web loyalty program, and developed a Google AdWords initiative. She actively contributes to the information security community and has served as a volunteer for the Grace Hopper Women in Computing Celebration (2017) and the Pace University GenCyber Program (2017-2018), has presented at r00tz Asylum at DEFCON25 (2017) and DEFCON26 (2018), Women in Cyber Security Conference (2017-2020), the Community College Cyber Summit (2018), and has guest lectured at multiple colleges and universities all across the country. Since 2017, Kaitlyn has served as the Chief Player Ambassador for the National Cyber League. She runs and regularly appears on their Thursday Night Live Coaching Sessions to encourage students nationwide to participate in CTF competitions to achieve their cybersecurity academic and career goals. Kaitlyn was also the grateful recipient of the Women in Cyber Security Conference 2019 Rising Leadership Award.
Certification and Training	Kaitlyn earned a Master of Science in Information Systems from Pace University in Pleasantville, NY in May of 2018 and holds a Certificate in Cybersecurity from Westchester Community College in Valhalla, NY. Kaitlyn also holds her CompTIA Security+ certification.
Tenure	Kaitlyn has been with Tevora since June 2018.

Troy Dahlin, Senior Consultant Federal and Third-Party Risk

Primary Role	As Tevora's Senior Consultant for Federal and Third-Party Risk practice areas. The Federal practice area provides clients with FISMA, FedRAMP, DFARS, NIST CSF and other related standards. Troy mentors consultants, manages client relationships, assists with pre and post sales activities, and oversees projects from the inception to the closeout presentation to ensure that every project exceeds client expectations.
Notable Accomplishments	Troy started in the Information Assurance field as a US Navy Information Systems Security Manager in 2001, responsible for the configuration and hardening of US Navy IT Assets meeting FISMA regulations and DITSCAP Accreditation process. Troy retired from the US Navy Reserve after 24 years of combined Active and Reserve duty as an IT Chief Petty Officer having performed as the Senior Enlisted Leader for two different units (Inshore Boat Unit 25 and Beach Master Unit 2). Troy's last duty station was Commander Navy Cyber Command (US Tenth Fleet) in Ft. Meade, MD. In 2017 he started work as the Corporate ISSM implementing and managing the RMF implementation within the company and supporting DoD and Federal customers. Also, with the implementation of the DFARS/ CMMC within the Corporate network he was the primary expert on implementation activities. As the Corporate ISSM, he was also responsible for incident handling, insider threat mitigation, investigations, self-assessments and managing COMSEC transfers.
Certification and Training	Troy holds the Certified Information Systems Security Professional (CISSP), CompTIA Security+, GIAC Certified Incident Handler (GCIH) certifications and earned a Bachelor of Science degree in computer networks and security from University of Maryland University College (2017).
Tenure	Troy has been with Tevora since the beginning of 2020.

Go forward. We've got your back.

Compliance – Enterprise Risk Management – Data Privacy – Security Solutions – Threat Management