SSP Secrets

Foundation for CMMC Assessment

Uday Ali Pabrai & Josh Williams

Global AI Cyber Defence Thought Leaders

Topics

Introduction

The System Security Plan (SSP) is a fundamental documentation of an organization's security posture. The SSP describes how an organization implements its security requirements. To develop an SSP that aligns with the requirements of the Cybersecurity Maturity Model Certification (CMMC), a structured approach must be followed. If an organization handles sensitive data, especially Controlled Unclassified Information (CUI), an SSP is required to comply with cybersecurity regulations. By following the guidelines and thoroughly documenting security practices, the organization can create a robust SSP that meets the stringent requirements of CMMC.

What is a System Security Plan?

> The SSP is a formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain supporting appendices or as references, other key security-related documents, such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.
>
> **CMMC Glossary and Acronyms - v2.0 | December 2021**

An SSP also addresses the following:

- Describes system boundaries and system environments of operation.
- Describes how security requirements are implemented and the relationships with or connections to other systems.

Being certified for CMMC means having a CMMC Third Party Assessor Organization (C3PAO) review an organization's SSP:

- To ensure it meets all the requirements for the CMMC level at which the organization is being assessed and;
- Verifying that the organization is doing everything it claims in the SSP.

SSP Components

The SSP describes the system environment, system responsibilities, and the current status of the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline controls required for the system. It also includes the Customer Implementation Summary/Customer Responsibility Matrix (CRM) that summarizes how each control is implemented and which party is responsible for maintaining that control that maps to the

NIST SP 800-171 requirements. Ensure Assessment Team Members are familiar with the CMMC Assessment Scope of the OSC and its SSP. NIST SP 800-18 provides guidance on developing security plans.

The SSP relates security requirements to a set of security controls. The SSP should contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended.

The SSP does not need to be a single document. It can be a collection of various documents including ones that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents—incorporating . This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

Federal agencies may consider the submitted SSP and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization. Organizations can document the SSP as separate or combined documents and in any chosen format.

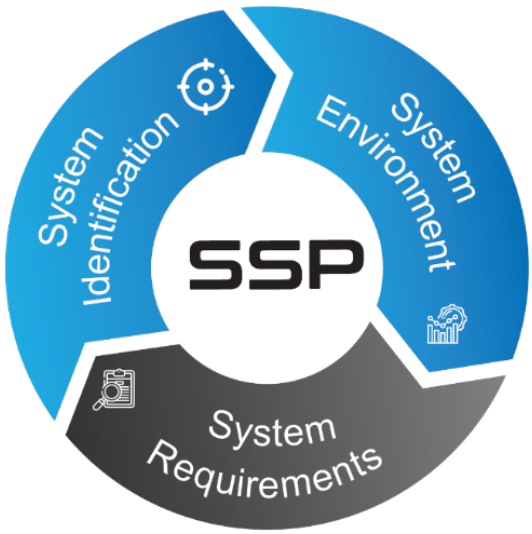


Figure 1: System Security Plan Components.

The SSP must include:

- Description of the CMMC Assessment Scope
    - High-level description of the assets.
- Description of the Environment of Operation

    - Physical surroundings in which an information system processes, stores, and transmits information.

- Identified and Approved Security Requirements
    - Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
- Implementation Method for Security Requirements
    - Description of how the identified and approved security requirements are implemented with the system or environment.
- Connections and Relationships to Other Systems and Networks.
- Defined Frequency of Updates (typically at least annually).
- General information system description (technical and functional description).
- Design philosophies
    - Defense-in-depth strategies and allowed interfaces and network protocols.
- Roles and responsibilities
    - Description of the responsibilities of key personnel, which may include the system owner, system custodian, authorizing officials, and other stakeholders.

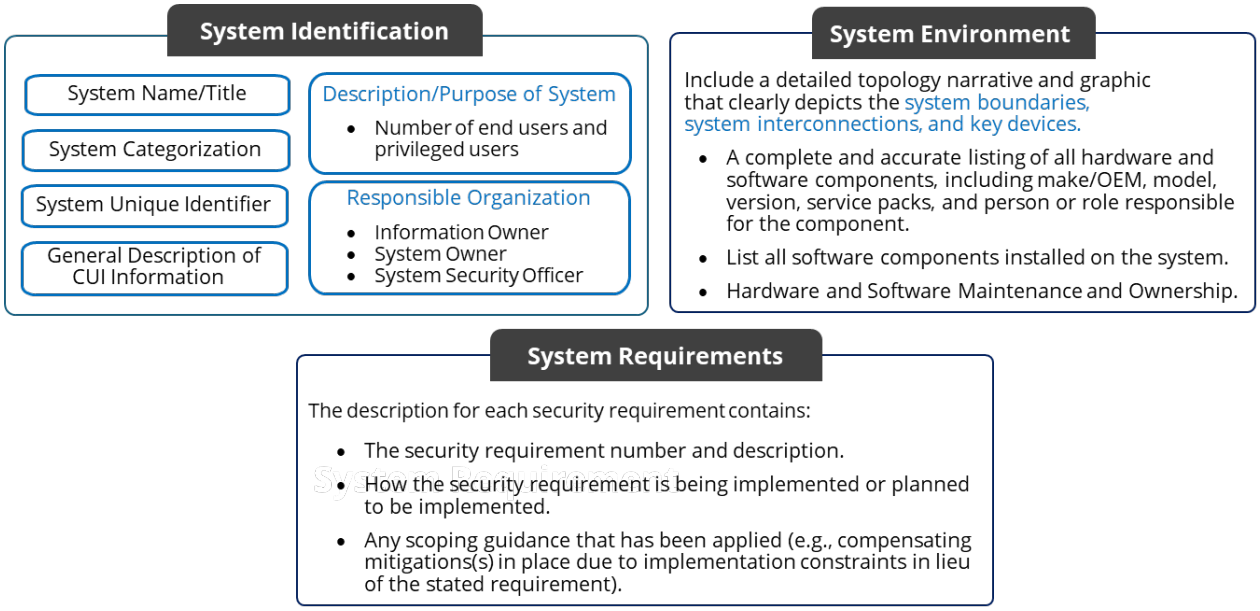


Figure 2: System Security Requirements.

OSA/OSC SSP Requirements

The Organization Seeking Assessment (OSA) or an Organization Seeking Certification (OSC) is required to document CMMC assets in the SSP to show they are managed using the OSA/OSC's

risk-based security policies, procedures, and practices, and accounted for within the OSA/OSC's CMMC Assessment Scope.

Review the SSP:

- If sufficiently documented, do not assess against other CMMC security requirements, except as noted below.
- If OSA/OSC's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies.
- The limited check(s) shall not materially increase the assessment duration or the assessment cost.
- The limited check(s) will be assessed against CMMC security requirements.

An OSA/OSC may use a FedRAMP Moderate (or higher) cloud environment to process, store, or transmit CUI in the execution of a contract or subcontract if the OSA/OSC ensures the Cloud Service Provider's offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012.

As part of the CMMC Assessment Scope, the security requirements from the CRM must be documented or referred to in the OSA/OSC's SSP, which will also be assessed. If the OSA/OSC utilizes an External Service Provider (ESP) other than a Cloud Service Provider (CSP), the ESP must have a CMMC Level 2 Certification as set forth in 32 CFR § 170.19(c)(2). If the ESP is internal to the OSA/OSC, the CMMC requirements being assessed should be listed in the OSA/OSC's SSP to show the connection to its in-scope environment.

SSP Scope

The SSP describes how the controls and solutions meet the security requirements. For the enhanced security requirements selected when the Advanced Persistent Threats (APTs) are a concern, articulated in NIST SP 800-172, the security plan provides traceability between threat and risk assessments and the risk-based selection of a security solution, including discussion of relevant analyses of alternatives and rationale for key security-relevant architectural and design decisions. This level of detail is important as the threat changes, requiring reassessment of the risk and the basis for previous security decisions.

When incorporating external service providers into the SSP, organizations state the type of service provided (e.g., software as a service, platform as a service), the point and type of connections (including ports and protocols), the nature and type of the information flows to and from the service provider, and the security controls implemented by the service provider.

For the safety of critical systems, organizations document situations for which safety is the primary reason for not implementing a security solution (i.e., the solution is appropriate to address the threat but causes a safety concern).

When solutions for implementing a requirement have differing levels of capabilities associated with their implementation, it is essential that the plan specifically document the rationale for the selected solution and what was acquired for the implementation. This information allows the organization to monitor the environment for threat changes and identify which solutions may no longer be applicable. While not required, it may also be useful to document alternative solutions reviewed and differing levels of risk associated with each alternative, as that information may facilitate future analyses when the threat changes.

In addition to the implementations required for CMMC Level 2 certification, which may not be risk-based, at Level 3, the SSP must carefully document the link between the assessed threat and the risk-based selection of a security solution for the enhanced security requirements (i.e., all CMMC L3 requirements are derived from NIST SP 800-172).

Examining CMMC SSP Requirements

In support of understanding and interpreting the CMMC Assessment Scope, the OSC must provide the Lead Assessor with supporting documentation, such as network diagrams, the SSP, policies, procedures, and organizational charts.

Each CMMC level demands progressively detailed and stringent SSP documentation, aligning security requirements with specific standards to ensure robust protection of sensitive information.

Security Assessment (CA): CA.L2-3.12.4 – System Security Plan

Develop, document, and periodically update SSPs that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

Assessment Objectives

Determine if:

[a] A SSP is developed.

[b] The system boundary is described and documented in the SSP.

[c] The system environment of operation is described and documented in the SSP.

[d] the security requirements identified and approved by the designated authority as non-applicable are identified.

[e] The method of security requirement implementation is described and documented in the SSP.

[f] The relationship with or connection to other systems is described and documented in the SSP.

[g] The frequency to update the SSP is defined.

[h] SSP is updated with the defined frequency.

Potential Assessment Methods and Objects

Examine:

- Security planning policy
- Procedures addressing SSP development and implementation
- Procedures addressing SSP reviews and updates
- Enterprise architecture documentation

This requirement, CA.L2-3.12.4, which requires developing, documenting, and updating SSPs, promotes effective information security within organizational systems required by SC.L2-3.13.2, as well as other system and communications protection requirements.

Risk Assessment (RA): RA.L3-3.11.4e – Security Solution Rationale

Document or reference in the SSP the security solution selected, the rationale for the security solution, and the risk determination.

Assessment Objectives

Determine if:

[a] The SSP documents or references the security solution selected.

[b] The SSP documents or references the rationale for the security solution.

[c] The SSP documents or references the risk determination.

Scenario

You are in charge of system security, optimally appointed so in writing. You develop the SSP and have senior leadership formally approve the document. The SSP explains how your organization handles CUI and defines how that data is stored, transmitted, and protected.

The criteria outlined in the SSP are used to guide the configuration of the network and other information resources to meet your company's goals. Knowing that it is important to keep the SSP current, you establish a policy that requires a formal review and update of the SSP each year.

Sample SSP

AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.

Control CUI Flow	

Responsible Role: Kate Koppenhoefer, Vice President & deputy General Counsel

Implementation Status (check all that apply):

☒ Implemented ☐ Not Applicable (N/A)
☐ Planned to be Implemented ☐ Inherited

Assessment Objective

The assessment objective of this practice Control CUI Flow (AC.L2-3.1.3), is to determine if:

[a] Information flow control policies are defined.
[b] Methods and enforcement mechanisms for controlling the flow of CUI are defined.
[c] Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.
[d] Authorizations for controlling the flow of CUI are defined.
[e] Approved authorizations for controlling the flow of CUI are enforced.

[a] Information flow control policies are defined:

- ABC Corp has a policy that dictates that users will be subject to disciplinary action for not following appropriate procedures.

[b] Methods and enforcement mechanisms for controlling the flow of CUI are defined:

- ABC Corp does not allow employees to upload FCI/CUI to SharePoint.
- ABC Corp does not allow employees to download files from Application on a non-ABC Corp managed computer.

[c] Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified:

- Only the System Owner is authorized to change the dataflow after approval from the CCB.

[d] Authorizations for controlling the flow of CUI are defined:

- Textual data is stored in the RDS database.
- Documents are stored in the private S3 buckets.
- Account or Group permissions (RBAC) (user vs admin) restrict access and movement of CUI. CUI resides within ABC Corp. ABC Corp does not have connections to other systems.
- CUI is labeled with DLP enabled.

[e] Approved authorizations for controlling the flow of CUI are enforced:

- Textual data is stored in the RDS database.
- Documents are stored in the private S3 buckets.
- Account or Group permissions (RBAC) (user vs admin) restrict access and movement of CUI. CUI resides within ABC Corp. ABC Corp does not have connections to other systems.
- CUI is labeled with DLP enabled.

Policy Reference: Control the Flow of CUI Policy

Procedure Reference: Control the Flow of CUI Procedure

Evidence Reference:

- 11102 Conditional Access.jpg
- 1308.docx
- 0417.01y-AWS_Prod_Inbound.png

Next Steps

The SSP is a foundational and culminating document within the CMMC framework, encapsulating an organization's cybersecurity posture and detailing how security requirements are met. By adhering to the guidelines outlined in the CMMC assessment, organizations can ensure that their SSPs are comprehensive, effectively mitigating risks and enhancing overall security resilience. The detailed documentation of security controls, risk assessments, policies, and continuous monitoring processes are essential for achieving and maintaining the required CMMC certification level.

Be prepared! Your assessor could ask to,

- EXAMINE security planning policy.
- INTERVIEW personnel with security planning and system security plan implementation responsibilities.
- TEST organizational processes for system security plan development, review, update, and approval.

References

CMMC Assessment Guide Level 2 | 2.0

CMMC Glossary and Acronyms

CMMC Assessment Guide Level 2 | 2.11

CMMC_Assessment_Guide_Level3 | 2.11

Global AI Cyber Defense Thought Leader

MSEE | CISSP (ISSAP | ISSMP) | CMMC (CCA, CCP, PA, PI, RPA, RP) | HITRUST® CCSFP | Security+

ISACA TOP-RATED SPEAKER

U.S. Department of Defense CMMC Program

Mr. Ali Pabrai, a global AI cybersecurity & compliance expert, is the chairman & chief executive of ecfirst. A highly sought after professional, he has successfully delivered solutions to U.S. government agencies, IT firms, healthcare systems, legal & other organizations worldwide. His career was launched with the U.S. Department of Energy's nuclear research facility, Fermi National Accelerator Laboratory. He has served as vice chairman and in several senior officer positions with NASDAQ-based firms.

Mr. Pabrai has led numerous engagements worldwide for ISO 27001, PCI DSS, NIST, CMMC, GDPR, CCPA, FERPA, HITRUST CSF and HIPAA/HITECH. Mr. Pabrai served as an Interim CISO for a health system with 40+ locations.

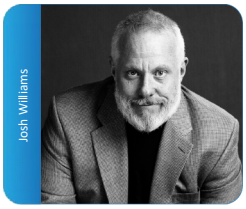
Mr. Pabrai has presented passionate briefs to tens of thousands globally, including the USA, United Kingdom, France, Taiwan, Singapore, Canada, India, UAE, Saudi Arabia, Philippines, Japan, Ireland, Bahrain, Jordan, South Africa, Egypt, Ghana and other countries.

He is a globally renowned speaker who has been featured as a keynote as well as moderated cybersecurity conferences. Mr. Pabrai is the author of several published works. Clients that Mr. Pabrai has delivered to have included the U.S. Defense Intelligence Agency (DIA), and the U.S. Naval Surface Warfare Center.

Mr. Pabrai was appointed and served (2017) as a member of the select HITRUST CSF Assessor Council. Mr. Pabrai is a proud member of the InfraGard (FBI).

"We have had the true pleasure of working with Ali Pabrai at conferences all over the world during the past few years - with one unanimous word that keeps resounding among audiences and staff alike - AWESOME!"
Michael Mach | *Conference Program Manager* | *ISACA*

ISACA Trust in, and value from, information systems



FEDSHARK

A cyber security practitioner with strong technical and leadership experience in both the public and private sectors, including information warfare engagements against GSFG, the Pakistani Hackers Club, the Chinese Communist Party, and Russia-affiliate BlackCat/ALPHV.

Classified and unclassified publication credits, including for NSF Award ACI-1626338 with Oak Ridge National Laboratory. Currently senior SME for regional healthcare network comprising 32 hospitals, 700 sites of care, multiple health centers, physician practices, rehab locations and other outpatient care locations in eastern Pennsylvania and NJ; implemented first private Full Operating Capability of the MITRE ATT&CK Framework for threat hunting. Most recently, Vice President of Security for a global IT Infrastructure Solutions, Data Storage and Cloud Services firm headquartered in the Fort Meade, MD area.

Provided subject matter expertise and multi-source fusion for incidence response and remediation including against the nation-state maleficent Yu Pingan responsible for the OPM breach. Created and operationalized a Cybersecurity Apprenticeship Program. Prior, managing principal of a DC-area management-consulting firm which crafted the first ever HIGH baseline for FedRAMP. SME for global DHS-component mission. Technical lead for regional integration and optimization effort to securely fuse Operational Technology input, GIS, modeling and simulation and multi-source sensors into a Common Operating Picture. PMO task lead for global implementation of anti-terrorism security and technology packages for Operational Technology and Critical Infrastructure. Corporate director of technology and engineering for winner of Contractor of the Year 6 consecutive years; architected security and support solutions for various DoD and federal civilian agencies; senior manager responsible for overall development and operations, intrusion protection and incident handling for multiple DoD networks, spearheaded successful defense and forensic analyses of focused cyber-attacks; lead element commander for DoD's only tactical TECHINT and MASINT unit, successfully responding to more than 173 National Intelligence Requirements during eight operational deployments.

"Mr. Williams' expertise in fusing the classic Intelligence Preparation of the Battlespace discipline with cyber operations resulted in identified and closed gaps in the enterprise RMF, increased maturity of our GRC posture, and significantly improved signal-to-noise optics and cyber situational awareness."
Scott S. | *DISL* | *IC Component*

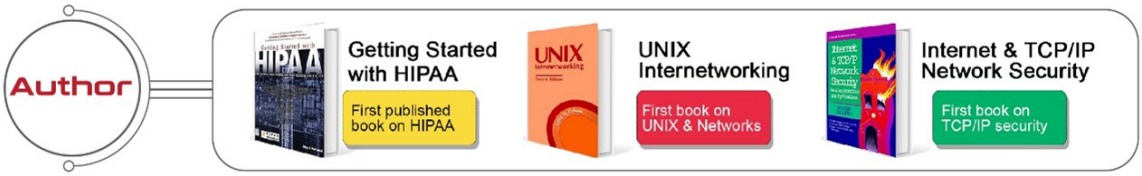
FBI Conference

"On behalf of the Idaho InfraGard (FBI), I would like to thank Pabrai for presenting at our conference. Pabrai is the kind of speaker you want to bring to executives and staff. He says it in a simple, no nonsense way, in a manner that everyone can understand."
Rachel Zahn | *President | InfraGard (FBI) | Idaho Alliance*

"You delivered a fantastic presentation and we all felt your passion for cyber security."
James E Lamadrid | *Supervisory Special Agent | Federal Bureau of Investigation (FBI) Cyber Task Force*

"Thank you Pabrai. Your enthusiasm and relevance for the Information Security material you presented at our combined Infragard (FBI) conference in Idaho Falls was very well received and pertinent to both our chapter as an organization and the constituents in attendance."

"As a government employee, I appreciated the simplified insight of highlighting the importance of compliance and funding compared to information security success beyond qualitative metrics. I heard many times over that your specific information with measurable results made your material directly relevant to individuals, businesses and organizations. Thanks again and I hope you are able to join us again in the future."
Clark Harshbarger | *FBI*



HITRUST® Authorized External Assessor | r2 HITRUST CERTIFIED