

Version <X.Y>

<Date>

Prepared for:

<Organization>

Prepared by:

<Author(s)>

Contract: <Contract ID>

<Other Front Matter>

<Organization-specific legal boilerplate, if applicable>

For Internal <Organization> Use. This document was prepared for authorized distribution only. It has not been approved for public release.



This document is derived from  
*MITRE Adaptive Capabilities Testing (ACT)™*.  
act.mitre.org | act@mitre.org

<Organization>

MITRE Adaptive Capabilities Testing (ACT)™

System Security Plan (SSP)  
Development Guide

Record of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Responsible Author | Description of Change |
| 1.0 | May 30, 2025 | Stefan DeShazo | Initial release of MITRE ACT templates and work aids. |

**Note to the Author Using this Template:**

This is a *template* for producing a MITRE ACT template tailored to your specific organization. Everything in this template can and should be customized by you to meet your organization’s specific needs and objectives.

Various objects and sections of text throughout the template are highlighted – these are **items that are very likely to require customization**, but you are free and encouraged to **edit the entire document and process** to suit your organization’s needs. By documenting your actual ACT process (including how it deviates from the baseline herein) in this template you are ensuring that your ACT assessments are consistent, repeatable, and can be accurately compared to assessments from other organizations’ implementations of ACT.

Table of Contents

[1. Introduction 1](#_Toc199102460)

[1.1 How To Use This Guide 1](#_Toc199102461)

[2. SSP Development Process Flowchart 1](#_Toc199102462)

[2.1 Identify Initial Roles 2](#_Toc199102463)

[2.2 Document System Information 2](#_Toc199102464)

[2.3 Identify System/Infrastructure Points of Contact (POCs) 3](#_Toc199102465)

[2.4 Define the Authorization Boundary 3](#_Toc199102466)

[2.5 Document the System Configuration 4](#_Toc199102467)

[2.6 Document the Compliance with Security Controls 4](#_Toc199102468)

[2.7 Finalize and Approve the SSP 5](#_Toc199102469)

# 

# Introduction

A System Security Plan (SSP) documents protection of an information system. The MITRE Adaptive Capabilities Testing (ACT) framework encourages and facilitates the creation of the SSP and its use in ongoing operations and in compliance and risk assessment activities performed under ACT and other assessment frameworks.

The purpose of the SSP is to:

* Provide an overview of the security requirements of the information system
* Describe the security controls in place or planned for meeting security requirements
* Delineates responsibilities and expected behavior of all individuals who access the information system

The SSP is important because it:

* Ensures a documented understanding of the boundary of an information system
* Documents components reside within the boundary of your system
* Documents data residing on your information system and how it will be protected during use

The SSP should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the organization’s senior information security officer.

Additional information not explicitly included in the SSP template or guidance may be included in the SSP, and the structure and format may be organized according to the organization’s needs, so long as the major sections described in this guide are adequately covered and readily identifiable.

## How To Use This Guide

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 defines the SSP as the “formal document that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements”.[[1]](#footnote-2)

This guide provides high-level assistance with creating a SSP under the MITRE ACT framework. It is intended to be used in conjunction with the *ACT SSP template* and with *NIST SP 800-18* (which provides low-level details). For more detailed information on the overall ACT process, please consult the *MITRE ACT Assessment Handbook*.

The SSP should be created during the initial development of a system; must be updated following any significant changes as determined by the Authorizing Official (AO); and must be updated on a recurring basis to document the system's evolution over time.

# SSP Development Process Flowchart

The flowchart in Figure 1 below shows the high-level steps used to develop an SSP document for an information system. The other subsections in Section 2 provide additional detail and guidance about these steps.

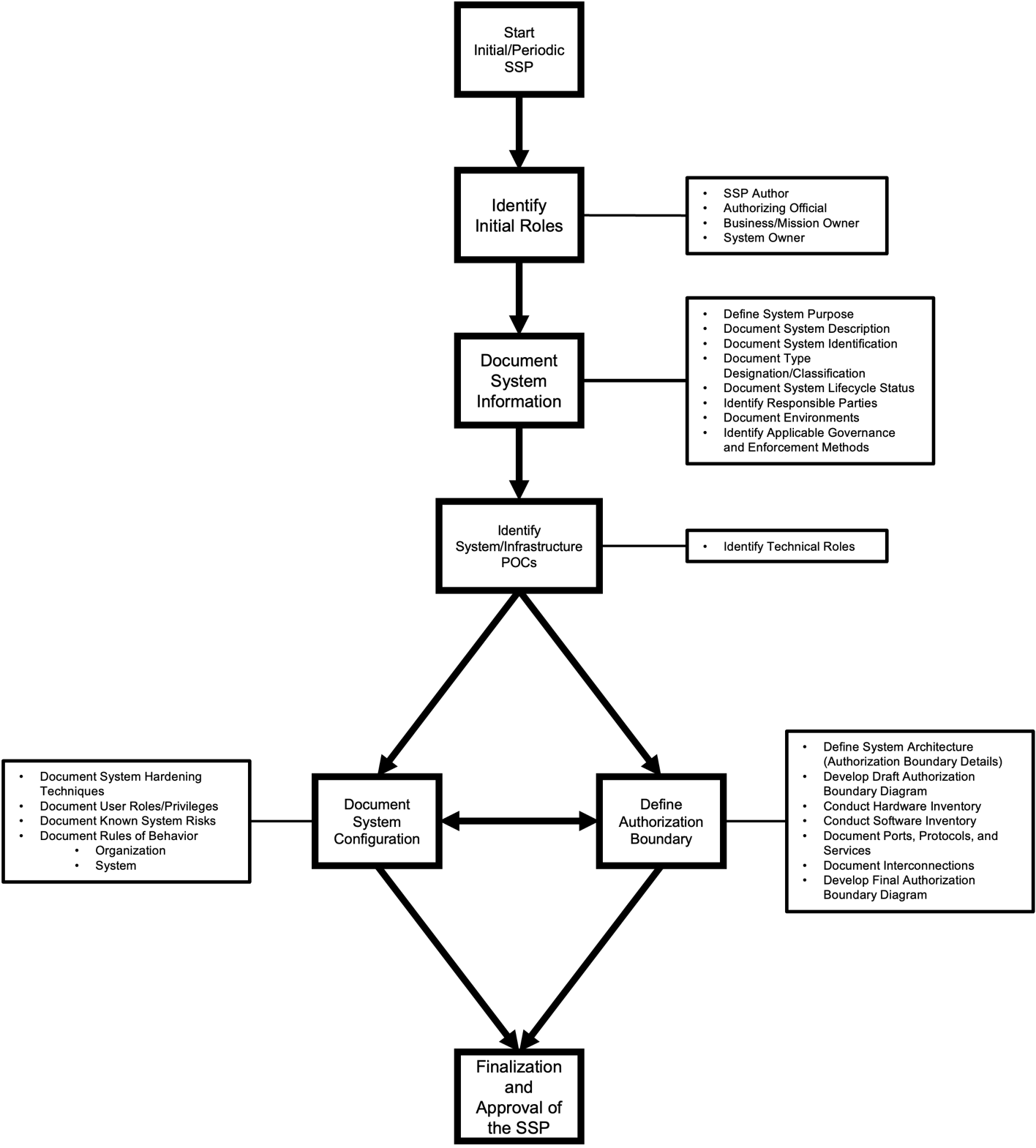


Figure 1. SSP Development Process Flowchart

## Identify Initial Roles

Before work can begin on developing the SSP, necessary roles must be identified. These include the following roles with brief explanations of each.

Table . Initial Roles

|  |  |  |
| --- | --- | --- |
| SSP Section | Role | Description |
| Change Log | SSP Author | Responsible for continuously collecting and updating the SSP. An Information System Security Officer/Manager[[2]](#footnote-3) (ISSO/ISSM) can typically fulfill this role, however, the SSP Author does not need to be an ISSO/ISSM. |
| 2.8.2.1 | Information System Security Officer / Manager (ISSO/ISSM) | Responsible for the security of the information system. |
| 2.8.3.1: Business / Mission Owner | Business and/or Mission Owner | Responsible for the business and/or mission process to which the information system contributes and understands the information system purpose. |
| 2.8.1 | System Owner | Has overall responsibility for ensuring that the information system meets Business/Mission needs. Oversees the development and day-to-day operation of the system. Is aware of the large-scale business and/or mission needs of the system. |
| 2.8.3.2 | System Developer / Maintainer | Executes development and/or day-to-day operational tasks on behalf of the System Owner. |
| 2.8.1: Responsible Organizations | Authorizing Official (AO) | Responsible for the security of all information systems within the organization and determines whether the information system meets organizationally defined requirements to operate at an acceptable level of risk. The AO is the only role authorized to accept risk on behalf of the organization. |

## Document System Information

After the initial roles have been identified, the next step is to document the essential information of the information system. This is outlined by the following tasks along with brief explanations**:**

Table . System Information

|  |  |  |
| --- | --- | --- |
| SSP Section | Information | Description |
| 2.1 | Define the Purpose | Provides insight into the overall goals of the information system and guides all other actions related to the information system. |
| 2.2 | Document the Description | Explains what the information system does and how it functions at a high level. |
| 2.3 | Provide Official Identification | Assigns the official information system name and nomenclature, along with any official and/or unique organizational identification number(s) or acronym(s). |
| 2.4 | Document Type Designation / Classification | Lists the system’s type, security category, FIPS categorization, sensitivity and/or classification level, and access requirements. |
| 2.5 | Document Operational Status | Lists the current operational state of the information system (New, Operational, Under Development, Undergoing a Major Modification, etc.), and may also document important security-related milestones. |
| 2.8 | Identify Responsible Parties | Assigns appropriate stakeholders for the information system and ensures their contact information is readily available. |
| 2.10 | Identify Applicable Governance and/or Enforcement Method(s) | Assigns regulations the information system must adhere to and how adherence will be ensured. |

## Identify System/Infrastructure Points of Contact (POCs)

After documenting the high-level information on the information system, the SSP Author can proceed to identifying the technical personnel involved with the information system. This identification process accelerates data gathering by allowing parallel lines of effort. Once the personnel are identified, the SSP Author can delegate task(s) of collecting essential technical data to them, aligning assignments with their respective areas of expertise. This approach facilitates a more efficient and comprehensive data collection process.

## Define the Authorization Boundary

This portion of the SSP development process provides more specific component meta-data of the information system, thereby facilitating a precise delineation of the authorization boundary[[3]](#footnote-4) and any pertinent supporting information. This process includes the following tasks along with brief explanations:

Table . Authorization Boundary Definition Tasks

|  |  |  |
| --- | --- | --- |
| SSP Section | Task | Description |
| 2.6 | Define System Architecture | This outlines the basic setup of the system and any associated information flows without specific details of information system components. |
| 2.6 | Develop the Draft Authorization Boundary Diagram | Provides a clear, unambiguous visual representation of the full set of logical and/or physical components that comprise the monolithic “thing” that will receive Authority to Operate (ATO) from the AO. |
| 2.7.1, 2.7.2 | Compile Hardware and Software Inventories | Provides the full inventory of every hardware and software component inside the Authorization Boundary. |
| 2.7.3 | Document Ports / Protocols / Services | Details all applications, protocols, and services (with their associated network ports) used within the Authorization Boundary. A Ports, Protocols, and Services (PP&S) list provides support to:   * Acquisition and Development * Certification/Authorization/Accreditation * Enterprise, Organization, and/or System Designated Accrediting Authority (DAA) * NetOps & Firewall Administrators * Perimeter and boundary defense * Connection approval processes |
| 2.7.5 | Document all Interconnections | Details all data flows into and out of the Authorization Boundary. |
| 2.6 | Develop the Final Authorization Boundary Diagram | The information collected by the SSP Author and any assigned delegates will be used to provide specific component information and, if needed, refine or redefine the Authorization Boundary. |

## Document the System Configuration

This portion of the SSP development process provides the configuration details of the information system. As with the process of developing the authorization boundary, the SSP Author and any assigned delegates can collect this information simultaneously. This process includes the following tasks along with brief explanations:

Table . System Configuration Definition Tasks

|  |  |  |
| --- | --- | --- |
| SSP Section | Task | Description |
| 2.7.4 | Document System Hardening Techniques | Identifies methods utilized to harden**[[4]](#footnote-5)** the information system. These methods may be accomplished manually or automatically by a variety of methods and/or tools including specific Security Technical Implementation Guide(s) (STIG)s, system hardening guides, secure development guides, analysis software used, etc. |
| 2.7.6 | Document User Roles / Privileges | Identifies an inventory of all authenticated user roles (admin, supervisor, user, etc.) in the information system and privileges (read, create, edit, delete, etc.) of each. |
| 2.9 | Document Rules of Behavior | Identifies rules of behavior prescribed by external and/or internal organizational authorities and additional rules added specifically for the information system. This may be divided into two separate lines of effort: *Organizational Rules of Behavior* and *System Rules of Behavior*. |

## Document the Compliance with Security Controls

This portion of the SSP development process provides low-level details about the specific ways in which the various applicable security controls (or other requirements) are implemented by the information system, the information system’s personnel, the owning organization, or how the implementations are inherited from other information systems or organizations.

Table . Security Control Compliance Documentation Tasks

|  |  |  |
| --- | --- | --- |
| SSP Section | Task | Description |
| 3 | Document the Compliance with Security Controls | The implementation details must be clearly mappable to each specific security control (or other requirement), and vice versa. |

## Finalize and Approve the SSP

Once all the information has been collected and verified by the SSP Author and any assigned delegates, the SSP Author compiles the information and finalizes the SSP. The SSP Author ensures no information is missing and represents the most accurate and current state of the information system. This SSP is then sent for approval by the appropriate authority. If not approved, the SSP Author coordinates with the appropriate information system technical experts for any additions and/or edits and updates the SSP for approval. Once approved, the SSP version is recorded in the changelog along with a detailed description of all updates.

1. The SSP is defined in detail in NIST SP 800-18. [↑](#footnote-ref-2)
2. “Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program”. See [NIST SP 800-18 Rev. 1](https://doi.org/10.6028/NIST.SP.800-18r1) under Information System Security Officer from CNSSI 4009 - Adapted [↑](#footnote-ref-3)
3. “All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.” See [NIST SP 800-39](https://doi.org/10.6028/NIST.SP.800-39) under Authorization Boundary. [↑](#footnote-ref-4)
4. “A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.” See [NIST SP 800-152](https://doi.org/10.6028/NIST.SP.800-152). [↑](#footnote-ref-5)