**Planning (PL)**

**PL-1: Security Planning Policy And Procedures**

NIST SP 800-53 Objective: The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]:

a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Control Translation: Ensure security planning policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the security planning policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Security Planning Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**PL-2: System Security Plan**

NIST SP 800-53 Objective: The organization:

a. Develops a security plan for the information system that:

- Is consistent with the organization’s enterprise architecture;

- Explicitly defines the authorization boundary for the system;

- Describes the operational context of the information system in terms of missions and business processes;

- Provides the security category and impact level of the information system including supporting rationale;

- Describes the operational environment for the information system;

- Describes relationships with or connections to other information systems;

- Provides an overview of the security requirements for the system;

- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Reviews the security plan for the information system

c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Control Translation: This control reviews the SSP and how the organization reviews and updates the plan. It is mostly a checklist of items that the SSP covers and documentation of the reviews. This control is related to PM-1 (Information Security Program Plan), PM-7 (Enterprise Architecture), PM-8 (Critical Infrastructure Plan), PM-9 (Risk Management Strategy), PM-11 (Mission/Business Process Definition).

Notes: Each item on the checklist can be used as a part of the answer and then the assessor can just explain where each of those items are covered.

How to test and evaluate: Review the security planning policy, procedures addressing security plan development and implementation, procedures addressing security plan reviews and updates, enterprise architecture documentation, security plan for the information system, records of security plan reviews and updates looking for each of the required checklist type items and for documentation of SSP reviews and updates performed on a regular schedule.

Technology specific: General

**PL-4: Rules of Behavior**

NIST SP 800-53 Objective: The organization:

a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and

b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Control Translation: This control is fairly simple and is just looking for documentation of rules of behavior for the system and acknowledgement of these rules from each user. This control is related to PS-6 (Access Agreements).

Notes: This may be documented in a larger procedure or via a specific rules of behavior document the acknowledgement of these rules may be a part of the reviewed rules or it may be a separate process. Most likely a sample of these agreements will need to be collected.

How to test and evaluate: Review the security planning policy, procedures addressing rules of behavior for information system users, and rules of behavior documents as well as examples of user acknowledgement of the rules to verify that the rules are both communicated and agreed to by each user.

Technology specific: General

**PL-5: Privacy Impact Assessment**

NIST SP 800-53 Objective: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

Control Translation: The privacy impact analysis should be completed and documented easily by reviewing the completed form.

Notes: Make sure there is a current PIA or that no changes to the system have happened that would necessitate a new PIA.

How to test and evaluate: Review the security planning policy, procedures addressing privacy impact assessments on the information system, privacy impact assessment looking for a completed PIA and any updates that might be needed.

Technology specific: General

PL-6: Security-Related Activity Planning

NIST SP 800-53 Objective: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Control Translation: This control is reviewing for security assessments, audits, system hardware and software maintenance, and contingency plan testing and exercises. Reviewing for both emergency and non-emergency situations.

How to test and evaluate: Review the security planning policy and procedures addressing security-related activity planning for the information system including the output of the most recent contingency plan testing and exercises, any output from hardware and software maintenance activities, and the most recent assessments or audits.

Technology specific: General