**System and Services Acquisition (SA)**

**SA-1: System and Services Acquisition Policy and Procedures**

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

a. A formal, documented system and services acquisition policy that includes information security considerations and 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 system and services acquisition policy and associated system and services acquisition controls.

Control Translation: Ensure system and services acquisition policy and procedures are in place.

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

How to test and evaluate: Examine SSP and System and Services Acquisitions 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

**SA-2: Allocation of Resources**

NIST SP 800-53 Objective: The organization:

a. Includes a determination of information security requirements for the information system in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and

c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Control Translation: This control is looking for specific budgeting and planning for security resources and equipment as a discrete part of the system budget. It also looks for analysis as to what is needed prior to purchasing. This control is related to PM-3 (Information Security Resources) and PM-11 (Mission/Business Process Definition).

How to test and evaluate: Review system and services acquisition policy, procedures addressing the allocation of resources to information security requirements, and organizational programming and budgeting documentation looking for documentation of a specific security line item and a rationale for this line item and the amount allocated.

Technology specific: General

**SA-3: Life Cycle Support**

NIST SP 800-53 Objective: The organization:

a. Manages the information system using a system development life cycle methodology that includes information security considerations;

b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and

c. Identifies individuals having information system security roles and responsibilities.

Control Translation: This control is looking for the existence of an SDLC and some specific items that the SDLC covers. There should be both roles and responsibilities and specific security roles defined in this document. This control is related to PM-7 (Enterprise Architecture).

Notes: It is possible that the organization or system will have a standard SDLC process that they follow. If this is the case they will have to prove how they assign overall roles and responsibilities as well as specific security roles within the system and outside of the SDLC that they are using.

How to test and evaluate: Review the system and services acquisition policy, procedures addressing the integration of information security into the system development life cycle process, and information system development life cycle documentation looking for the defined SDLC processes they are following and the roles and responsibilities definitions contained within.

Technology specific: General

**SA-4: Acquisitions**

NIST SP 800-53 Objective: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

a. Security functional requirements/specifications;

b. Security-related documentation requirements; and

c. Developmental and evaluation-related assurance requirements.

Control Translation: This control is looking for specific inclusions in acquisition contracts such as any functional requirements for the security of the system, the documentation that accompanies the functional requirements, and any other requirements that relate to assessment of the system from a security perspective.

How to test and evaluate: Review the system and services acquisition policy, procedures addressing the integration of information security requirements and/or security specifications into the acquisition process, and acquisition contracts for information systems or services looking for defined specifications or requirements that the organization needs as well as the documentation for these specifications.

Technology specific: General

**SA-5: Information System Documentation**

NIST SP 800-53 Objective: The organization:

a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:

- Secure configuration, installation, and operation of the information system;

- Effective use and maintenance of security features/functions; and

- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and

b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:

- User-accessible security features/functions and how to effectively use those security features/functions;

- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and

- User responsibilities in maintaining the security of the information and information system; and

c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Control Translation: This control is looking for documentation of the information system including configuration guides, user guides, and security notifications. This information may be public in the case of COTS or sensitive in other cases. This documentation can also include overall configuration for a system that is made up of many sub-components and software. For information that is proprietary the organization should document attempts to obtain the documentation as well as when the documentation is unavailable or nonexistent.

Notes: Frequently this documentation consists of COTS product manuals which are publicly available. If the organization has developed their own software or used GOTS or other not widely available solutions, look for documentation and the sensitivity levels associated.

How to test and evaluate: Review the SSP, the system and services acquisition policy, procedures addressing information system documentation, information system documentation including administrator and user guides, records documenting attempts to obtain unavailable or nonexistent information system documentation.

Technology specific: All

**SA-6: Software Usage Restrictions**

NIST SP 800-53 Objective: The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Control Translation: This control is looking for a list of approved software, software licenses and terms, examples of a system used to track installed software and licenses used, and documentation of peer-to-peer file sharing controls within the system.

Notes: Even if peer-to-peer file sharing is not allowed there should be some documentation or a configuration example for how the system monitors for this activity.

How to test and evaluate: Review the system and services acquisition policy, procedures addressing software usage restrictions, site license documentation, list of software usage restrictions, centralized software installation management, configuration of network monitoring systems, system security plan looking for evidence that software installations are tracked and peer-to-peer software is monitored or controlled.

Technology specific: All

**SA-7: User-Installed Software**

NIST SP 800-53 Objective: The organization enforces explicit rules governing the installation of software by users.

Control Translation: This control is looking for implementation of installation rules. This could be blocking users from installing anything and having privileged users that are responsible for installs, a centralized mechanism that manages licenses and applications, or a policy that recommends rules but does not directly enforce. This control is related to CM-2 (Baseline Configuration).

Notes: Make sure to look for both sides of the equation, the rules governing installation of software as well as the enforcement of those rules.

How to test and evaluate: Review the system and services acquisition policy, procedures addressing user installed software, list of rules governing user installed software, and network traffic on the information system.

Technology specific: All

**SA-8: Security Engineering Principles**

NIST SP 800-53 Objective: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Control Translation: The control is asking for assurance that the organizational components were designed using security principles.

How to test and evaluate: Test this control last and reference previous testing to include actual screenshots and system level documentation. Review the SDLC methodology and any developer security guidance or requirements. The key is to show and prove that each component was either designed with or without security principles. Use the testing results to make this determination. The best testing results would be from CM-2, CM-6, CM-7, AC-7, AU-8, etc. (utilize many of the technical test cases).

Technology specific: General

**SA-9: External Information System Services**

NIST SP 800-53 Objective: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Monitors security control compliance by external service providers.

Control Translation: This control is to ensure that if external provides of organization security services are being utilized (third party contractors working on behalf of the organization such as a help desk); the contractors must adhere to the same security requirements as the organization.

How to test and evaluate: Obtain the last test performed by the organization. Review the test to ensure the third party organization meets the organization defined requirements. Review any contracts with external organizations to ensure that they include language describing security requirements and compliance.

Technology specific: All

**SA-10: Developer Configuration Management**

NIST SP 800-53 Objective: The organization requires that information system developers/integrators:

a. Perform configuration management during information system design, development, implementation, and operation;

b. Manage and control changes to the information system;

c. Implement only organization-approved changes;

d. Document approved changes to the information system; and

e. Track security flaws and flaw resolution.

Control Translation: This control is to ensure that organization developers are tracking the changes made to the organization components.

Notes: This control is related to CM-3 (Configuration Change Control), CM-4 (Security Impact Analysis), and CM-9 (Configuration Management Plan).

How to test and evaluate: Utilize the screenshots and artifacts collected during CM-3, CM-4, CM-5, and SI-2 testing to show the process. New screenshots will need to be collected for the development devices. Select two development devices per unique component to show that changes to the development device changes are tracked. This will more than likely occur through a ticketing system.

Technology specific: All

**SA-11: Developer Security Testing**

NIST SP 800-53 Objective: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):

a. Create and implement a security test and evaluation plan;

b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and

c. Document the results of the security testing/evaluation and flaw remediation processes.

Control Translation: This control is to ensure that developers or organizational components test the component, identify flaws, and remediate the flaws.

Notes: This control is related to S-A-10, CA-5, and SI-2.

How to test and evaluate: Many components in the development stage do not records flaws and track them properly. This could be a potential easy failure. Obtain evidence from two development devices per unique component type. The evidence should detail a flaw being found (user reported or scan issue most likely), the tracking of the flaw, the remediation actions, and the scan or user test to show the flaw has been corrected.

Technology specific: All

**SA-12: Supply Chain Protection**

NIST SP 800-53 Objective: The organization protects against supply chain threats by employing an organization-defined list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy.

Control Translation: This control is to ensure that all purchased organizational items and devices follow a pre-determined chain of custody and actions to ensure that all property is accounted for and only approved acquisitions occurs.

How to test and evaluate: Test this control by collecting five purchase orders. Collect the tickets to show the actions associated with purchase orders. Examine organization and component level documentation to determine the organization defined measures to ensure proper chain of acquisitions. Compare the artifacts to the policy to ensure proper compliance with organizational requirements.

Technology specific: General

**SA-13: Trustworthiness**

NIST SP 800-53 Objective: The organization requires that the information system meets the organization defined level of trustworthiness.

Control Translation: This control is to ensure the organizational components are designed with the a layer of trust. The intent of this control is to ensure that organizations recognize the importance of trustworthiness and making explicit trustworthiness decisions when designing, developing, and implementing organizational information systems.

Notes: This control is related to RA-2 (Security Categorization), SA-4 (Acquisitions), SA-8 (Security Engineering Principles), and SC-3 (Security Function Isolation).

How to test and evaluate: Examine organization and component level documentation to determine the organization defined level of trustworthiness. Test this control by utilizing previous artifacts already collected. The goal is to show that tickets are used to track changes, no unauthorized access can occur, the information within the organizational components is secure, the access control lists are accurate, and the audit logs are investigated for unusual activity. All of these previously performed tests will be able to show a level of trust. Utilize the determined level of trust and compare that level to the organizational level.

Technology specific: General