**Risk Assessment (RA)**

**RA-1: Risk Assessment Policy And Procedures**

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

a. A formal, documented risk assessment 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 risk assessment policy and associated risk assessment controls.

Control Translation: Ensure risk assessment policy and procedures are in place.

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

How to test and evaluate: Examine SSP and Risk Assessment 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

**RA-2: Security Categorization**

NIST SP 800-53 Objective: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Control Translation: This control is usually looking for a FIPS 199 security categorization document to have been completed. If this is not the document completed there should be other documentation of the perceived impact level of the system in question along with rationale for the level. This control is related to CM-8 (Information System Component Inventory), MP-4 (Media Storage), SC-7 (Boundary Protection).

Notes: A signed FIPS 199 categorization should be the document found to satisfy this.

How to test and evaluate: Review the signed FIPS 199 categorization, the risk assessment policy, any procedures addressing security categorization of organizational information and information systems, and the security plan.

Technology specific: General

**RA-3: Risk Assessment**

NIST SP 800-53 Objective: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results;

c. Reviews risk assessment results at an organization-defined frequency; and

d. Updates the risk assessment at an organization-defined frequency or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Control Translation: This control is looking for a risk assessment process to be completed either as a part of regular security audits or as a part of another process (e.g. continuous monitoring or audits as a result of changes).

Notes: Documentation can be an outcome of the audit or as a supporting document to the audit report.

How to test and evaluate: Review the risk assessment policy, security planning policy and procedures, procedures addressing organizational assessments of risk, security plan, or risk assessment for analysis and reporting of system risks.

Technology specific: General

**RA-5: Vulnerability Scanning**

NIST SP 800-53 Objective: The organization:

a. Scans for vulnerabilities in the information system and hosted applications at an organization-defined frequency and/or randomly in accordance with organization-defined process and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;

- Formatting and making transparent, checklists and test procedures; and

- Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities within organization-defined response times in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Control Translation: This control is looking for a procedure and method to be used to scan systems on a regular frequency as well as when deemed necessary. The ideal assessment nets the documented procedures, outputs showing the procedures being followed and a documented review of outputs. This control is related to CA-2 (Security Assessments), CM-6 (Configuration Settings), RA-3 (Risk Assessment), SI-2 (Flaw Remediation).

Notes: Make sure that all devices from the sample are reflected in the scan results. In addition check to ensure that the scan results show a secured system or a system improving over time.

How to test and evaluate: Review the risk assessment policy, procedures addressing vulnerability scanning, security plan, vulnerability scanning results (e.g. Nessus reports, FoundStone report output, and/or other scanning mechanisms), and patch and vulnerability management records showing review and addressing issues found during scans.

Technology specific: Some portion apply to all components and some potions will be at the general level