For High-Impact Information Systems

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

RA-1.1 - Examine risk assessment policy and procedures; other relevant documents or records **and**

Interview organizational personnel with risk assessment responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents risk assessment policy and procedures;	S			
(ii)	The organization disseminates risk assessment policy and procedures to appropriate elements within the organization;				
(iii)	Responsible parties within the organization periodically review risk assessment policy and procedures; and				
(iv)	The organization updates risk assessment policy and procedures when organizational review indicates updates are required.	S			

RA-1.2 - Examine risk assessment policy and procedures; other relevant documents or records **and**

Interview organizational personnel with risk assessment responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The risk assessment policy addresses purpose, scope, roles and responsibilities management commitment, coordination among organizational entities, and compliance;				
(ii)	The risk assessment policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(iii)	The risk assessment procedures address all areas identified in the risk assessment policy and address achieving policy-compliant implementations of all associated security controls.				

RA-2 SECURITY CATEGORIZATION - The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

RA-2.1 - Examine risk assessment policy; procedures addressing security categorization of organizational information and information systems; security planning policy and procedures; FIPS 199; NIST Special Publication 800-60; information system security plan; other relevant documents or records, **and**

Interview organizational personnel with security categorization and risk assessment responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization conducts the security categorization of the information system as an enterprise-wide exercise with the involvement of senior-level officials including, but not limited to, authorizing officials, information system owners, chief information officer, senior agency information security officer, and mission/information owners;				
(ii)	The security categorization is consistent with FIPS 199 and NIST Special Publication 800-60;				
(iii)	The organization considers in the security categorization of the information system potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts;				
(iv)	The organization includes supporting rationale for impact-level decisions as part of the security categorization; and				
(v)	Designated, senior-level organizational officials review and approve the security.				

RA-3 RISK ASSESSMENT - The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

RA-3.1 – Examine risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; NIST Special Publication 800-30; other relevant documents or records, **and**

Interview organizational personnel with risk assessment responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization assesses the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support its operations and assets (including information and information systems managed/operated by external parties); and				
(ii)	The risk assessment is consistent with the NIST Special Publication 800-30.				

RA-4 RISK ASSESSMENT UPDATE - The organization updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

RA-4.1 - Examine risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; information system security plan (for organization-defined frequency for risk assessment updates); records of risk assessment updates; NIST Special Publication 800-30; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of risk assessment updates;				
(ii)	The organization updates the risk assessment in accordance with the organization-defined frequency or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system;				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(iii)	The risk assessment update is consistent with the NIST Special Publications 800-30; and				
(iv)	The revised risk assessment reflects the needed changes based on the organization's experiences during security plan implementation.				

RA-5 VULNERABILITY SCANNING - The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.

RA-5.1 – Examine risk assessment policy; procedures addressing vulnerability scanning; risk assessment; information system security plan (for organization-defined frequency for vulnerability scanning); vulnerability scanning results; patch and vulnerability management records; other relevant documents or records **and**

Interview organizational personnel with risk assessment and vulnerability scanning responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of vulnerability scans within the information system;				
(ii)	The organization scans for vulnerabilities in the information system in accordance with the organization-defined frequency or when significant new vulnerabilities affecting the system are identified and reported:				
(iii)	The organization uses appropriate scanning tools and techniques to conduct the vulnerability scans including those tools that ensure interoperability among tools and automate parts of the vulnerability management process by using standards for (a) enumerating platforms, software flaws, and improper configurations, (b) formatting and making transparent checklists and test procedures, and (c) measuring vulnerability impact;				
(iv)	The organization performs network vulnerability scanning in accordance with NIST Special Publication 800-42; and				
(v)	The organization handles patch and vulnerability management in accordance with NIST Special Publication 800-40.				