Select Step – Management Perspective

Selecting and specifying the **appropriate security controls for information systems** to meet the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is accomplished following the guidelines in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. The use of security controls from NIST SP 800-53 and the incorporation of tailored baseline controls as a starting point in the control selection process, **facilitate a more consistent level of security across federal information systems and organizations**. It also offers the needed **flexibility to appropriately modify the controls** based on specific organizational policies and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk.

Risk Executive (Function)

Organizations need a **comprehensive approach to manage risk—an approach that recognizes the balance between the organization's mission and business functions and its day-to-day operations—including the use of information systems** to achieve their missions and accomplish their business goals. The management of organizational risks can best be achieved by the implementation of an overall risk executive (function). The **risk executive (function) provides senior leadership input and oversight for all risk management and information security activities across the organization** (e.g., security categorizations, common security control identification, continuous monitoring, and reauthorization) to help ensure consistent risk acceptance decisions.

Organizational Support

An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business processes and the information systems and organizational infrastructure supporting those processes. Senior leadership (i.e., risk executive (function), chief information officer, senior information security officer, authorizing officials, mission/business owners, information owners/stewards, information system owners) involvement in the security control selection process is essential to ensure that there is a **commitment to the risk mitigation decisions** that are made during the Select Step since senior leaders will be accountable for the resulting risk that will be incurred by the organization.

Organizations should **provide specific policies and guidance on the types of security control tailoring and supplementation activities that are permissible and appropriate** for the information systems supporting the organization. The tailoring and supplementation decisions made during the selection of the security controls can potentially impact large segments of the organization and affect the organization's security state and risk posture.

FIPS 200

FIPS 200 specifies the **minimum security requirements for the information and information systems** supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements in a consistent and repeatable manner.

NIST SP 800-53

NIST SP 800-53 provides **guidelines for selecting and specifying security controls and minimum assurance requirements** that enable organizations to protect their information systems. NIST SP 800-53, Appendix F, provides a **master catalog of security controls** than can be effectively used to mitigate risk and demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. Appendix E describes the minimum assurance requirements for security controls for low-, moderate-, and high-impact systems. It is the **responsibility of the organization to select the appropriate security controls and minimum assurance requirements** for their information systems.

Information System Owner

The security controls are **selected by the information system owner** based on the security categorization of the information system. The security control selection process includes, as appropriate: (i) choosing a set of baseline security controls; (ii) tailoring the baseline security controls by applying scoping, parameterization, and compensating control guidance: (iii) supplementing the tailored baseline security controls, if necessary, with additional controls or control enhancements to address unique organizational needs based on a risk assessment and local cost-benefit analyses, or special circumstances; and (iv) specifying minimum assurance requirements, as appropriate.

Security Control Baselines

Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of an organization demonstrates the organization's commitment to security and that due diligence is exercised in protecting its information and information systems. **Baseline controls are the minimum security controls recommended for an information system based on the system's security impact level. Three sets of baseline controls have been identified** corresponding to the low-, moderate-, and high-impact levels defined in the security categorization process.

Risk Assessment

Risk assessments provide important inputs in determining whether the security controls in the tailored baseline adequately protect the organization's operations, assets, and individuals as well as other organizations, and the Nation. The security control tailoring and supplementation activities that are conducted during the Select Step are based on the results of a current risk assessment to determine whether the tailored and supplemented set of security controls can sufficiently mitigate the identified risks to the information system.

Tailoring

Organizations have the flexibility to tailor, or adjust, the initial security control baselines to address specific mission and business processes, organizational requirements, and operational environments. Tailoring activities include the application of appropriate scoping guidance to the initial baseline (e.g., determining whether or not a security control that addresses a specific information technology applies to a particular information system); the specification of compensating security controls, if needed, to employ in lieu of a recommended security control; and the specification of organization-defined parameters values (e.g., the frequency of incident response testing) in the security controls that require one or more organization-defined values.

Supplementing The Baseline

Organizations also have the flexibility to supplement the tailored security controls. The final determination of the security controls necessary to provide adequate security is a **function of an organizational assessment of risk and the resulting trustworthiness required for the information systems** used in carrying out the organization's mission/ business processes to sufficiently mitigate this risk. In many cases, additional security controls or control enhancements may be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations that an initial or tailored security control does not sufficiently address.

Use Restrictions

There may be situations in which an organization discovers it is employing information technology beyond its ability to adequately protect critical or essential missions. That is, **the organization cannot apply sufficient security controls within an information system to adequately reduce or mitigate mission risk**. In those situations, **an alternative strategy is needed to protect the mission from being impeded**—a strategy that considers the mission risks that are being brought about by an aggressive use of information technology. One such alternative strategy is to employ restrictions on the information that an information system can process, store, or transmit or the manner in which a mission or business function is automated.

Assurance

Assurance is the **grounds for confidence that the security controls implemented within an information system are effective in their application**. Assurance can be obtained in a variety of ways including the actions taken by the developers and implementers of an information system's security controls (e.g., tracing security function requirements to software code, testing incident response procedures) and the methods and actions taken by security control assessors (e.g., comprehensive testing of a critical automated security control implementation). NIST SP 800-53, Appendix E, describes the minimum assurance requirements associated with low-, moderate-, and high-impact systems. Organizations should **provide specific policies and guidance on the types of assurance measures that should be implemented to meet those minimum assurance requirements**.

Continuous Monitoring of Security Controls

A critical aspect of risk management is the ongoing monitoring of security controls employed within or inherited by the information system. An effective monitoring strategy is developed early in the system development life cycle and can be included in the security plan. **The continuous monitoring strategy identifies the security controls to be monitored, the frequency of monitoring, and the control assessment approach. The strategy defines how changes to the information system will be monitored, how security impact analyses will be conducted, and the security status reporting requirements.** The approval of the monitoring strategy can be obtained in conjunction with the security plan approval.

System Security Plan

The **security controls along with the supporting rationale for selection decisions and any information system use restrictions are documented in the security plan** for the information system. Documenting in the security plan any significant risk management decisions in the security control selection process is imperative in order for authorizing officials to have the **necessary information to make credible, risk-based decisions** regarding the authorization of organizational information systems. In addition, without such information, the understanding, assumptions, and rationale supporting those important risk decisions will, in all likelihood, not be available when the state of the information systems or environments of operation change, and the original risk decisions are revisited.

References

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*[1], Expected March 2011
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010
- NIST SP 800-39, Final Public Draft, *Managing Risk from Information Systems: An Organizational Perspective*, December 2010
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009
- Select Step FAQs, www.csrc.nist.gov//groups/SMA/fisma/Risk-Management--Framework/select/index.html

[1] The first public draft of NIST SP 800-30, Revision 1 is expected in early 2011, which will focus on risk assessment.