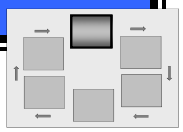
CATEGORIZE STEP – MANAGEMENT PERSPECTIVE

NIST RISK MANAGEMENT FRAMEWORK



Security categorization is the most important step in the Risk Management Framework and affects information security decisions both for the organization and individual information systems and influences all remaining steps in the Risk Management Framework—from the selection of security controls to the level of effort needed to assess and maintain the controls. Security categorization uses FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, to **assess the criticality and sensitivity of the information and information system to determine the system's security impact level**. Security categorizations should be reviewed on an ongoing basis to help ensure that mission and business impact assessments reflect the current organizational priorities and operational environments.

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 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) to help ensure consistent risk acceptance decisions.

SENIOR LEADERSHIP

Senior leadership oversight in the security categorization process is essential so that the subsequent steps in the Risk Management Framework can be carried out in an effective manner. An error in the initial categorization process can result in either an over-specification or under-specification of the security controls for the information systems. Over-specification of security controls means that the organization is spending more on information security than is actually necessary and potentially taking resources away from other mission/business areas with greater protection needs. Under-specification of security controls means that selected mission/business processes may be at greater risk due to the insufficient protection measures allocated for the information systems supporting those processes.

ORGANIZATIONAL SUPPORT

Organizations should conduct FIPS 199 security categorizations of information types and associated information systems as an organization-wide activity with the participation and involvement of senior leaders and other key officials within the organization (e.g., officials executing or participating in the risk executive (function), mission and business owners, information system owners, information security managers, information system security officers, chief information officers, senior agency information security officers, and authorizing officials) and others external to the organization when needed and appropriate. Conducting the security categorization process as an organization-wide exercise helps ensure that the process **accurately reflects the criticality, sensitivity, and priority of the information systems that are supporting organizational mission/ business processes**.

FIPS 199

FIPS 199 defines security categories for both information and information systems. **The security categories are based on the potential "worst-case" impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization** to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

POTENTIAL IMPACT VALUES

FIPS 199 defines **three levels of potential impact on organizations or individuals** should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The use of these definitions takes place within the context of each organization and the overall national interest. The potential impact values are:

- **Low** – the loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations and assets, individuals, other organizations, and the Nation.
- **Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations and assets, individuals, other organizations, and the Nation.
- **High** – the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations and assets, individuals, other organizations, and the Nation.

INFORMATION TYPES

Information is categorized according to its information type. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories,* divides information into two major activity areas—information associated with an organization's mission-specific activities and information associated with administrative, management, and support activities common to most organizations. The **information types are based on the lines of business defined in the Federal Enterprise Architecture** (FEA) for these two activity areas.

CATEGORIZING INFORMATION TYPES

Information types are categorized by looking up the recommended impact value (e.g., low, moderate, high, or not applicable) for the confidentiality, integrity, and availability security objectives of each identified information type from the appendices in NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* or the organization's supplement to NIST SP 800-60 of additional, organization-specific information types. After the recommended security objective impact values are determined, they can be adjusted based on legislation, Executive Orders, regulations, or system use.

CATEGORIZING INFORMATION SYSTEMS

The highest impact value for each security objective from all of the system's information types in the information system is the system's security category. For an information system, the overall impact level is the highest value (i.e., high water mark) of the three security objectives in the system's security category. This high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. The determination of the information system's impact level must be accomplished prior to the consideration of minimum security requirements and the selection of appropriate security controls for the information system.

SECURITY CONTROLS

When addressing the security considerations for their information systems, organizational officials must ask **"What security controls[1] are needed to adequately protect the information systems that support the operations and assets of the organization in order to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?"** Security categorization answers this question and associates minimum security controls and minimum assurance requirements with each security impact level. **By selecting the appropriate security controls and minimum assurance requirements, the organization is demonstrating a**

[1] Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information.

commitment to security and ensures that due diligence is exercised in protecting their information and information systems.

REFERENCES

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes I & II*, August 2008
- NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008
- NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008
- Categorize FAQ, www.csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/categorize/index.html

Draft