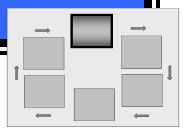
# CATEGORIZE STEP – ORGANIZATIONAL PERSPECTIVE



## NIST RISK MANAGEMENT FRAMEWORK

Organizations need a comprehensive approach for addressing risk—an approach that provides greater visibility into and understanding of the integrated operations and business flows of the organization. The categorization process is the first step in implementing this risk management approach. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines requirements for categorizing information and information systems. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance in assessing the criticality and sensitivity of the information and associated information system to determine the system's security category (i.e., potential worst case impact from loss of confidentiality, integrity, and availability) and overall impact level.

In order to effectively support information owners/information system owners, the organization's information security program office needs to establish relationships with other organizational entities, develop organization-wide categorization guidance, prepare a catalog of organization-specific information types, lead organization-wide categorization sessions, and serve as the organizational point of contact for information owners/information system owners throughout the categorization process.

**NOTE: The *Organizational Perspective* is provided as one example of how SP 800-60 may be implemented to categorize federal information and information systems in accordance with FIPS 199. Readers should understand that other implementations may be used to support their particular circumstances.**

The organizational perspective in this document elaborates on the basic steps and guidance in NIST SP 800-60 as examples for stimulating ideas in implementing an organization-wide categorization process.

### ESTABLISH RELATIONSHIPS WITH ORGANIZATIONAL ENTITIES

The success of the Risk Management Framework is dependent upon the collaboration among the organization's many entities. Working together, senior leaders can make information risk decisions that ensure the organization's mission and business activities remain functional while also maintaining an acceptable security posture. The information security program office reaches out to the organization's information owners/information system owners to provide adequate guidance and direction on the categorization process. In addition, the information security program office develops and maintains relationships with the enterprise architecture group, the Capital Planning and Investment Control (CPIC) personnel, and the technical operations personnel.

### DEVELOP ORGANIZATION-WIDE CATEGORIZATION GUIDANCE

The information security program office should develop categorization guidance that supplements the guidance in NIST SP 800-60 and provides organization-specific procedures and documentation, approval, and reporting requirements. The organization-specific guidance should address how information owners/information system owners; (i) integrate the categorization process into the system development life cycle; (ii) handle new information types; (iii) conduct the categorization process for their individual information systems; (iv) document the categorization decision in the system security plan; (v) gain approval for the categorization decision; (vi) report the categorization decision; and (vii) maintain the categorization decision by periodically validating that the categorization decision has not changed.

## PREPARE THE ORGANIZATION'S SUPPLEMENT TO NIST SP 800-60

The categorization process begins with a thorough analysis of the organization's mission and business processes integrated with the organization's enterprise architecture to identify the types of information processed, stored, and transmitted by the information systems supporting those processes. The security categorization process draws on the organization's enterprise architecture to provide traceability from the Federal Enterprise Architecture (FEA) reference models through the segment and solution architectures to the individual information systems within the organization.

The information security program office determines if there are any organization-specific information types unique to their organization. The organization's missions and lines of business are reviewed to identify information types that are not included in NIST SP 800-60, Volume II. For each organization-specific information type, the information security program office determines the provisional security impact value (low, moderate, or high) of each of the security objectives (confidentiality, integrity, and availability) and any special factors regarding the impact determination. Each organization-specific information type should be documented in a supplement to NIST SP 800-60 of additional, organization-specific information types following a structure and format similar to NIST SP 800-60, Volume II.

## LEAD THE ORGANIZATION-WIDE CATEGORIZATION SESSIONS

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

If an organization chooses to implement the categorization process without conducting organization-wide categorization sessions, it should still ensure that the impact levels for information systems are consistent throughout the organization. Categorization consistency can be achieved by providing training sessions to individual information owners/ information system owners and reviewing and approving the categorization decisions for individual information systems at a senior level (e.g., officials executing or participating in the risk executive function, chief information officer, or senior agency information security officers).

## 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
- Draft NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, April 2008
- Categorize FAQ, www.csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/categorize/index.html