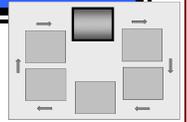


CATEGORIZE STEP – TIPS AND TECHNIQUES FOR ORGANIZATIONS

NIST RISK MANAGEMENT FRAMEWORK



The security categorization process is the first step in implementing a comprehensive approach for addressing risk. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, define 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, and for determining 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 and information owners/information system owners, the organization’s information security program office needs to establish collaborative relationships with other organizational entities, develop organization-wide categorization guidance, prepare a supplement to NIST SP 800-60 of additional, 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 risk management processes.

NOTE: The *Tips and Techniques for Organizations* are 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 tips and techniques for organizations in this document elaborate on the basic steps and guidance in NIST SP 800-60 as examples for stimulating ideas in implementing categorization standards and guidelines in organization-specific and information system-specific environments.

NIST SP 800-60 defines a four-step process for categorizing information and information systems as (i) identify information types, (ii) select provisional impact levels for the information types, (iii) review provisional impact levels and adjust/finalize information impact levels for the information types, and (iv) assign a system security category and overall impact level.

ESTABLISH RELATIONSHIPS WITH ORGANIZATIONAL ENTITIES

The success of the categorization process is dependent upon the collaboration among the organization’s many entities. Senior leaders must balance the benefits gained from using information systems with the risks that the same systems will be the vehicle through which adversaries cause mission or business failure. Working together, senior leaders can make informed decisions, provide adequate security, mitigate risk, and help ensure the organization’s missions and business activities remain functional.



DRAFT

Conduct Outreach to Information and Information System Owners

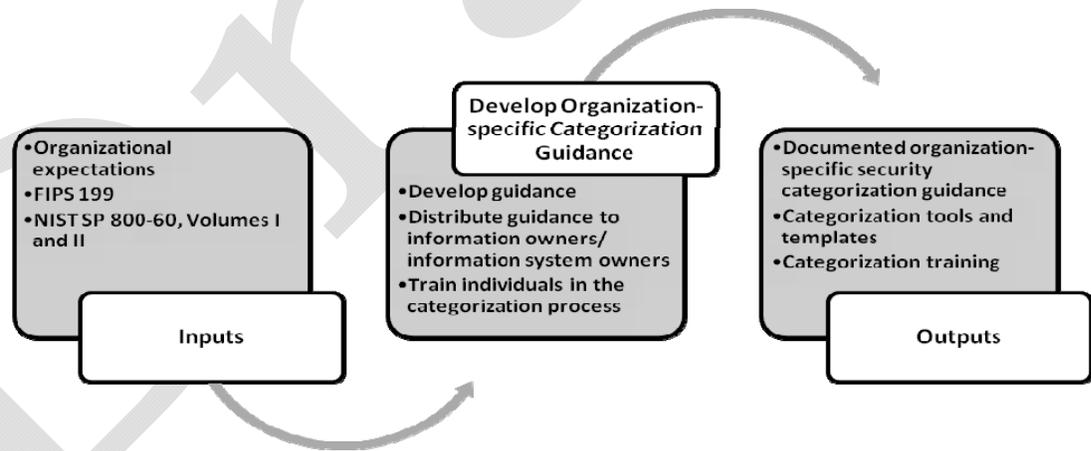
The information security program office should reach out to information owners/information system owners to provide them with the guidance and support they need to effectively and consistently implement the categorization process. The outreach activities should include providing detailed organizational categorization guidance, coordinating the definition and dissemination of organization-specific information types, leading organization-wide categorization sessions, providing training on the categorization process, developing templates or obtaining tools to support the process, and serving as the organizational point of contact.

Collaborate with Other Organizational Entities

The information security program office also collaborates with the enterprise architecture group to validate that the organization's information types are represented in the enterprise architecture. They work with the Capital Planning and Investment Control (CPIC) personnel to ensure there is adequate funding for the information system based on the system's impact level and that the system's security posture is maintained throughout the life cycle. The information security program office also collaborates with the technical operations personnel to validate that organizational security policies based on the system's impact level are implemented effectively, common security controls are implemented, and that a configuration management process exists that includes security in the operational decision making process.

DEVELOP ORGANIZATION-SPECIFIC CATEGORIZATION GUIDANCE

In order to ensure the categorization process is implemented consistently throughout the organization, the information security program office prepares organization-specific guidance that defines the categorization process, distributes the guidance to all individuals involved in the process, and provides appropriate training.



Develop Guidance

The organization's information security program office develops 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 addresses how information owners/information system owners:

- Integrate the categorization process into the system development life cycle;
- Handle new information types;
- Conduct the categorization process for their individual information systems;
- Document the categorization decision in the system security plan;
- Obtain approval for the categorization decision;

DRAFT

- Report the categorization decision; and
- Maintain the categorization decision.

When new systems are developed, the categorization decision is made during the initiation phase of the system development life cycle based on the mission/business needs of the organization. As a system proceeds through the development process, the categorization decision needs to be revisited based on changes to the information system or its environment. Once a system is operational (or is an existing operational system), the categorization decision needs to be evaluated periodically to confirm that the criticality/sensitivity of the system remains the same. If an operational system is scheduled for a significant update, the categorization process is repeated.

NIST SP 800-60, Volume II, provides a comprehensive list of information types that are consistent with the Federal Enterprise Architecture (FEA), but organizations may have additional information types (consistent with their organizational enterprise architectures). These additional information types need to be identified and validated at the organizational level. As an organization develops their own unique information types, those information types need to be documented, published in an organization's supplement to NIST SP 800-60, and shared with information owners/information system owners throughout the organization.

Each organization implements the NIST SP 800-60 categorization process that has been adapted for use within their organization. The organization-specific process should define any required documentation, approval, and reporting requirements. Organizationally provided tools and templates also enable information owners/information system owners to make consistent categorization decisions across the organization and increase collaboration and understanding among organizations that need to share the information.

Categorization decisions are maintained and updated as needed throughout the life cycle of the information system. As part of the continuous monitoring process, the information owner/information system owners monitor the security posture of the information system. Changes or activities that could affect the security of an information system include changes in the operating environment, new threats to the system, changes to the system functions, new interconnections, or added or removed information or information technology component. When changes to the information system are identified, the information owner/information system owner determines the extent to which those changes and ongoing activities affect the system's impact level by conducting a system security impact analysis of those changes.

Distribute Guidance to Information and Information System Owners

After the organization-specific categorization guidance has been prepared and approved, the guidance is distributed to all individuals within the organization involved in the categorization process. The distribution method could be through a website or security portal sponsored by the information security program office or through email and paper distribution to appropriate individuals within the organization. The most effective distribution method is one that ensures that the categorization guidance is widely available and easily obtainable by all individuals responsible for protecting the organization's information and information systems.

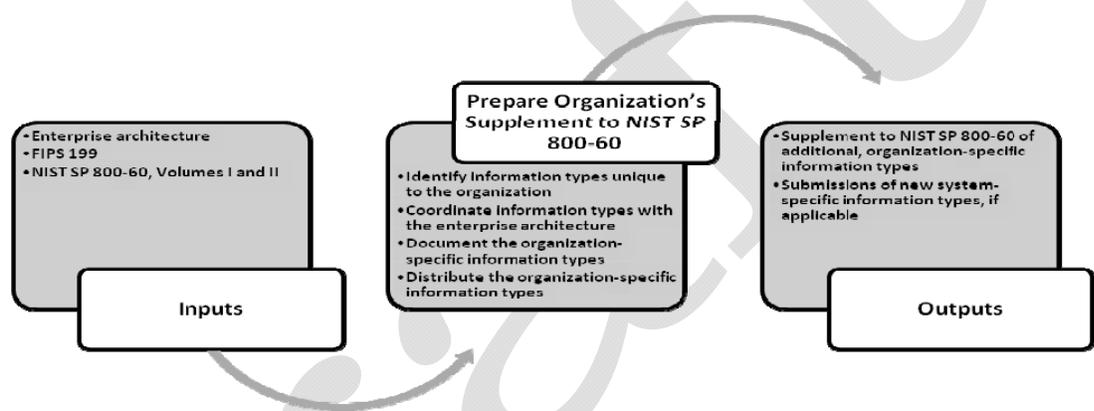
DRAFT

Train Individuals in the Categorization Process

In addition to distributing the organization-specific categorization guidance, the information security program office offers training to individuals involved in the categorization process. Training ensures that the organization-specific guidance and tools, templates, and techniques are applied consistently throughout the organization and that the individuals involved in the categorization process understand clearly how the categorization process has been implemented within the organization.

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

While NIST SP 800-60, Volume II, provides a comprehensive list of information types that are consistent with the FEA, organizations may also identify additional information types unique to their mission. These additional, organization-specific information types are identified, validated as consistent with the organization's enterprise architecture, documented, and distributed to the organization's information owners/information system owners for use in their information system categorization efforts.



Identify Information Types Unique to the Organization

The information security program office, in conjunction with the authorizing officials and the information owners/information system owners, may identify information types that are unique to the organization. To identify the unique, organization-specific information types, they must review the organization's Business Reference Model (BRM) and enterprise and segment architectures. The BRM documents the organization's missions and lines of business. If the organization has identified additional lines of business beyond those that are identified in the FEA BRM, there should be corresponding organization-specific information types associated with those additional lines of business and their supporting sub-functions.

Additional information types are also identified by reviewing the data elements in each individual information system. Every effort should be made to match the data elements to the existing information types in NIST SP 800-60—either by matching to a portion of the information type description or matching to an extension of the information type description. If the data elements cannot be matched to an information type from NIST SP 800-60, Volume II, a new information type has been identified.

Each unique information type identified for an individual information system should be shared with the organization's information security program office that will validate whether the information type is unique and consistent with the organization's enterprise architecture and add the information type to the organization's supplement to NIST SP 800-60 so that other information owners/information system owners can use the information type in their categorization efforts.

DRAFT

Coordinate Information Types with the Enterprise Architecture

To validate the organization-specific information types, the information security program office submits the proposed new information type to the organization's information security program office and enterprise architecture group who will determine whether the lines of business and supporting sub-functions are appropriate, used within the organization, and documented in the organization's enterprise and segment architectures.

Document the Organization-specific Information Types

After an organization-specific information type has been identified and approved for use within the organization, the information type is documented and shared with other individuals involved in the categorization process. While the documentation for the information type may follow any format, the descriptive information for each information type must be consistent with the descriptive information provided in NIST SP 800-60, Volume II:

- Information type title and brief description of the new organization-specific information type;
- Recommended security category; and
- For each security objective (confidentiality, integrity, and availability):
 - Discussion of the recommended security impact value assigned; and
 - Special factors affecting the impact value determination.

The impact values selected for the information type's security category should be consistent with the impact value descriptions from FIPS 199 and NIST SP 800-60 as summarized in the following table:

POTENTIAL IMPACT VALUES			
Security Objective	LOW	MODERATE	HIGH
<i>Confidentiality</i>	Limited adverse effect	Serious adverse effect	Severe or catastrophic adverse effect
<i>Integrity</i>	Limited adverse effect	Serious adverse effect	Severe or catastrophic adverse effect
<i>Availability</i>	Limited adverse effect	Serious adverse effect	Severe or catastrophic adverse effect

Distribute the Organization-specific Information Types

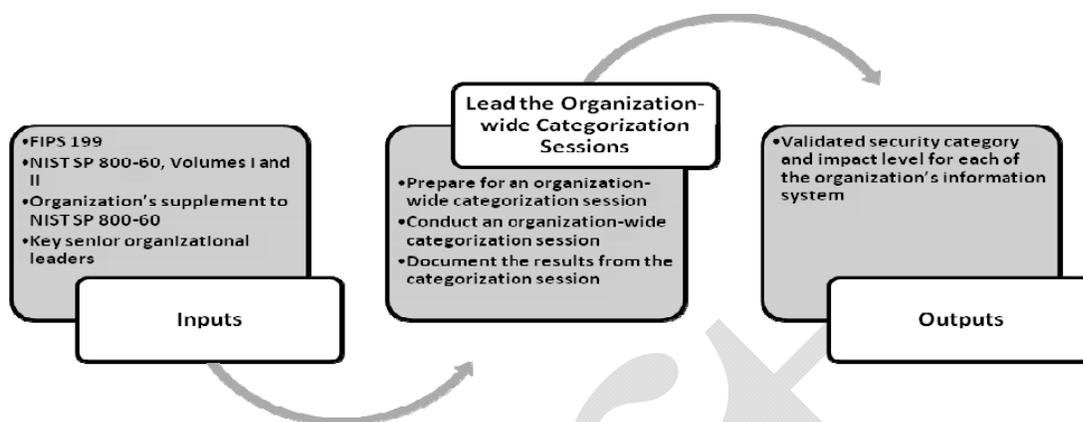
Updates to the organization's supplement to NIST SP 800-60 are distributed to all individuals involved in the categorization process to ensure that information owners/information system owners base their categorization or re-categorization efforts on up-to-date information.

LEAD THE ORGANIZATION-WIDE CATEGORIZATION SESSIONS

The information security program office is responsible for leading the organization-wide categorization sessions. These sessions should take a cooperative, problem-solving approach and bring together a diverse group of individuals to ensure that the organization's information and information systems are categorized consistently. Both the information security program office and the information owners/information system owners prepares for the organization-wide categorization session.

The information security program office is responsible for documenting the results of the session, sharing the results, and validating that the results have been implemented in the information system and in supporting documentation. If an organization does not conduct organization-wide categorization sessions, an alternate method should be implemented to ensure the categorization decisions are consistent throughout the organization.

DRAFT



Prepare for an Organization-wide Categorization Session

In order to effectively conduct an organization-wide categorization session, information owners/information system owners complete their initial security categorizations prior to the session. Each information owner/information system owner who participates in the session should have documented the following information in the system security plan:

- General and technical system descriptions, including the system boundary and interconnections with other information systems;
- List of the information types determined for the information system;
- Description of the organization-specific information types used in determining the information system's security category and security impact level;
- Provisional and adjusted security category for each information type; and
- System's security impact level for the information system.

The information security program office prepares to lead the organization-wide categorization session by completing the following:

- Arrange for physical facilities;
- Prepare agenda, description of session activities, and code of conduct for the categorization session;
- Collect organizational risks, including known vulnerabilities to share with participants;
- Identify and illustrate interconnections among organizational information systems;
- Consolidate initial categorization decisions for all information systems involved in the categorization session;
- Determine criteria for categorization consistency; and
- Develop guidance and other documentation (e.g., session hand-outs, instructions, templates) to be used during the session.

The information security program office serves as the facilitator of the organization-wide categorization session.

Conduct an Organization-wide Categorization Session

During the organization-wide categorization session, the information owners/information system owners for all (or a sub-set) of the organization's information systems validate whether their categorization decisions are consistent throughout the organization.

At the organization-wide categorization session, the information security program office begins by presenting the agenda, describing the session activities, and defining the session's code of conduct (e.g., listen to all points of view, adhere to a three-minute rule, record deferred issues and address them at a later time, etc.). As each information system is discussed, the group determines whether each information system's categorization decision

DRAFT

should be retained, increased, or decreased based on the perceived value of the information and information system to the organization and the potential impacts on the organization's mission, day-to-day operations, personnel, and assets if the information system was jeopardized due to a loss of the confidentiality, integrity, or availability of its information.

Document the Results from the Categorization Session

After the organization-wide categorization session is completed, the information security program office documents and shares the results of the session with the session participants and senior leaders within the organization. The information security program office is also responsible for validating that the decisions made in the categorization sessions have been incorporated into the affected information systems' functional and security documentation and implemented in the information systems.

CATEGORIZATION SUMMARY

Risk related to the operation and use of information systems is a component of organizational risk that senior leaders must address as a routine part of their ongoing risk management responsibilities. Categorizing information and information systems is the first step in this risk management process. The organization's information security program office is the group that coordinates the organization's information security activities and collaborates with other interrelated organizations to help achieve the organization's mission and business activities.

In order to effectively implement the organization's security categorization process, the information system program office establishes relationships with other organizations, prepares detailed categorization guidance for the organization that implements NIST SP 800-60, defines and documents any additional, organization-specific information types, and serves as the point of contact on all categorization issues within the organization.

The products resulting from the organization's implementation of the security categorization effort include the following:

- Guidance on how to implement the categorization process for the organization that is consistent with NIST SP 800-60
- Tools and templates to support the organization's categorization process
- Training on the organization's categorization process
- Supplement to NIST SP 800-60 of additional, organization-specific information types
- Results of the organization-wide categorization sessions

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