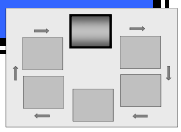
CATEGORIZE STEP – SYSTEM PERSPECTIVE



NIST RISK MANAGEMENT FRAMEWORK

Security categorization based on 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*, provides a structured way to assess the criticality and sensitivity (i.e., potential worst case impact from loss of confidentiality, integrity, and availability) of the information being processed, stored, and transmitted by an information system. The resultant categorization decision is used to select and tailor the security controls for the information system, using NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. Information owners/information system owners are responsible for categorizing their information systems.

NOTE: The *System 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.

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.

The system perspective in this document elaborates on the basic steps and guidance in SP 800-60 as examples for stimulating ideas in implementing categorization standards and guidelines in organization-specific and information system-specific environments.

PREPARE FOR SYSTEM SECURITY CATEGORIZATION

In order to prepare for the system security categorization process, the information owner/information system owner should:

1. Collect all relevant documentation specific to the information system.
2. Obtain the organization-specific documentation that includes a supplement to NIST SP 800-60 of additional, organization-specific information types, organization categorization policies and procedures, and preliminary risk assessment results.
3. Develop organizational relationships with the information security program office, enterprise architects, individuals involved in the capital planning and investment control process, cross-organizational stakeholders, and technical operations personnel.

IDENTIFY INFORMATION TYPES

The information owner/information system owner must identify the information types processed by, stored in, or transmitted by the information system and document them in the system security plan. To determine the information types for the system, the information owner/information system owner should:

1. Verify the characteristics of the system, including the system boundary, and the information that it processes, stores, or transmits.
2. Identify the data elements and how the data elements are used in the information system, group the data elements together in a logical way, and describe each data element group.
3. Match the data elements in the system to the available information types identified in the organization's supplement to NIST SP 800-60 of additional, organization-specific information types and NIST SP 800-60, Volume II. To

determine which information type is most relevant to each group of data elements, the information owner/information system owner should look at the context in which the information is used.

4. If the information system processes any information types not included in NIST SP 800-60, Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, or in the organization's supplement to NIST SP 800-60, document those information types following the NIST SP 800-60 or the organization-defined format and submit them to the information security program office for approval.
5. Document the information types identified for the system in the system security plan.

SELECT THE PROVISIONAL IMPACT VALUES FOR EACH INFORMATION TYPE

To determine the provisional, or initial, security impact values for an information system, the information owner/information system owner should:

1. Look up the provisional impact values for the three security objectives (confidentiality, integrity, and availability) for each identified information type using NIST SP 800-60 or the organization's supplement to NIST SP 800-60.
2. Document the provisional impact values for each information type in the system security plan.

ADJUST THE INFORMATION TYPE'S PROVISIONAL IMPACT VALUES

To adjust the information type's provisional impact values, the information owner/ information system owner should:

1. Review the appropriateness of the provisional impact values for each of the system's information types and adjust each impact value for each security objective based on the *special factors affecting impact determination* guidance in the organization's supplement to NIST SP 800-60 and NIST SP 800-60, Volume II. In many cases the impact values will not change.
2. Document the final impact values for each security objective for each information type in the system security plan and provide a justification for all adjustments

ADJUST THE SYSTEM'S PROVISIONAL SECURITY CATEGORY

To determine if the provisional security category is realistic, the information owner/ information system owner should:

1. Determine the provisional security category by identifying the highest value assigned to each security objective across all information types—that is, identify the maximum impact value for confidentiality, integrity, and availability and document the results in the system security plan.
2. Analyze the provisional security category to determine if it is realistic or if there is a need to increase one or more of the security objectives in the provisional security category. When adjusting the provisional security category, the information owner/information system owner considers factors such as an aggregation of the information processed, critical system functionality, extenuating circumstances, operational environment, characteristics of the information types, or availability needs of the system's information when making the security categorization decisions.
3. Document the adjusted security category in the security plan along with the justification for any adjustments.

Determine the Information System Security Impact Level

To determine the information system's security impact level, the information owner/ information system owner should:

1. Determine the highest value assigned to a security objective in the security category (i.e., the system's impact level).
2. Document the system's impact level in the security plan.

Obtain Approval for the System Security Category and Impact Level

Designated senior-level officials within the organization must review and approve the security categorization. To obtain approval for the system's security category and the impact level, the information owner/information system owner should:

1. Submit the system security plan with the categorization information and supporting justifications to the designated senior-level official.
2. Obtain approval of the information system categorization decision and document the approval in the system security plan.

Maintain the System Security Category and Impact Level

Periodically, the information owner/information system owner should reconfirm the criticality and sensitivity of the information system and its information. The information owner/information system owner should:

1. Monitor the information system (as part of the continuous monitoring process) and identify any changes planned or implemented in the information system.
2. Determine the extent to which the changes and ongoing activities affect the system's impact level by analyzing the effect on the system's security posture caused by the changes and activities.
3. If the system changes affect the impact level, the system categorization should be reviewed and any changes incorporated into the categorization documentation in the system security plan.
4. Submit the system's revised impact level to the appropriate organizational official for review and approval (or revision).

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, Volume 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