CATEGORIZE STEP FAQS

NIST RISK MANAGEMENT FRAMEWORK

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that promotes: (i) effective management and oversight of information systems and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress. The NIST security categorization standards and guidance are defined in 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*.

General Categorize FAQs

1. What is security categorization and why is it important?
2. How is the categorization decision used?
3. Who is responsible for categorizing each information system?
4. What is the relationship between categorization and the organization's enterprise architecture?
5. What is the risk executive function's role in the categorization process?
6. During which phase of the system development life cycle should a new system be categorized?
7. What are external information systems?
8. How does the categorization decision affect external information services?

Categorization Fundamentals

9. What is the difference, if any, between a security category and a security impact level?
10. How is the security category expressed?
11. What information is needed to categorize an information system?
12. What is an information system boundary?
13. When should the information system boundary be established?
14. Who establishes the information system boundary?
15. How is the information system boundary established?
16. What are the various types of information that government information systems process?
17. How is personally identifiable information (PII) handled during the categorization process?

Organizational Support for the Categorization Process FAQs

18. What is the organization's role in categorizing information systems?
19. How do organizations establish mission-based information types?
20. How does the information system categorization affect the use of common security controls?

System-specific Application of the Categorization Process FAQs

21. What are the steps to categorize an information system?
22. What are the potential security impact values?
23. How are the security categories of information types adjusted?
24. Can the system's security category be adjusted?
25. How is the overall security impact level of the information system determined?
26. Should an information system always be high-impact if at least one of its information types is categorized as high?
27. How should the information system categorization be documented?
28. Is it ever necessary to modify the security category of an information type?

General Categorize FAQs

1. What is security categorization and why is it important?

Security categorization provides a structured way to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system. The security category is based on the potential impact (worst case) to 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 and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions.[1] The information owner/information system owner identifies the types of information associated with the information system and assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type.

The high water mark concept is used to determine the security impact level of the information system for the express purpose of prioritizing information security efforts among information systems and selecting an initial set of security controls from one of the three security control baselines in NIST SP 800-53.[2]

2. How is the categorization decision used?

Once the overall security impact level of the information system is determined (i.e., after the system is categorized), an initial set of security controls is selected from the corresponding low, moderate, or high baselines in NIST SP 800-53. Organizations have the flexibility to adjust the security control baselines following the scoping guidance, using compensating controls, and specifying organization-defined parameters as defined in NIST SP 800-53. [3] The security category and system security impact level are also used to determine the level of detail to include in security documentation and the level of effort needed to assess the information system.[4]

3. Who is responsible for categorizing each information system?

Ultimately, the information owner/information system owner or an individual designated by the owner is responsible for categorizing an information system. The information owner/information system owner identifies all the information types stored in, processed by, or transmitted by the system[5] and then determines the security category for the information system by identifying the highest value (i.e. high water mark) for each security objective (confidentiality, integrity, and availability) for each type of information resident on the information system.[6]

[1] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 1

[2] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, p. 17

[3] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 32

[4] NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008, pp. 9-10

[5] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 16

[6] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 4

Organizations should conduct security categorizations as an organization-wide activity with the involvement of the senior leadership and other key officials within the organization.[7] Senior leadership oversight in the security categorization process is essential so that the Risk Management Framework can be carried out in an effective and consistent manner throughout the organization.

4. WHAT IS THE RELATIONSHIP BETWEEN CATEGORIZATION AND THE ORGANIZATION'S ENTERPRISE ARCHITECTURE?

The information types defined in NIST SP 800-60 are based on OMB's Business Reference Model (BRM) [8] as described in the *Federal Enterprise Architecture Consolidated Reference Model Document*.[9] The BRM provides a framework facilitating a functional (rather than organizational) view of the federal government's lines of business, including its internal operations and its services for citizens, independent of the organizations performing them.[10]

The BRM is structured into a tiered hierarchy representing the business functions of the government. Business areas are the highest level followed by lines of business, then the corresponding business sub-functions related to each line of business.[11] The business sub-functions from the BRM are the basic operations employed to provide the system services within each area of operations or line of business[12] and are the information types defined in NIST SP 800-60. Each federal agency is expected to apply the BRM from the Federal Enterprise Architecture to their specific organization.

5. WHAT IS THE RISK EXECUTIVE FUNCTION'S ROLE IN THE CATEGORIZATION PROCESS?

Organizations should include management of organizational risks from information systems as part of an overall risk executive function to address the issues related to managing risk and the associated information security capabilities that must be in place to achieve adequate protection[13] for the organization's information and information systems. The risk executive function helps ensure that information security considerations for individual information systems are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission/business processes.[14]

During the categorization process, the risk executive function provides the senior leadership input and oversight to help ensure consistent categorization decisions are made for individual information systems

[7] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 29

[8] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 14

[9] OMB, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007

[10] OMB, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007, p. 6

[11] OMB, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007, p. 26

[12] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. A-9

[13] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 12

[14] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 13

across the organization. The risk executive function facilitates the sharing of security-related and risk-related information among senior leaders to help these officials consider all types of risk that may affect mission and business success and the overall interests of the organization at large.[15]

6. DURING WHICH PHASE OF THE SYSTEM DEVELOPMENT LIFE CYCLE SHOULD A NEW SYSTEM BE CATEGORIZED?

The initial security categorization for the information and the information system should be done during the initiation phase of the system development life cycle along with an initial risk assessment. The initial risk assessment defines the threat environment in which the information system will operate and includes an initial description of the basic security needs of the system.[16]

Once the information system is operational, the organization should revisit, on a regular basis, the risk management activities described in the NIST Risk Management Framework, including the system categorization. Additionally, events can trigger an immediate need to assess the security state of the information system. If a security event occurs, the organization should reexamine the security category and impact level of the information system to confirm the criticality/sensitivity of the system in supporting its mission operations or business case. The resulting impact on organizational operations and assets, individuals, other organizations, or the Nation may provide new insights regarding the overall importance of the system in assisting the organization to fulfill its mission responsibilities.[17]

7. WHAT ARE EXTERNAL INFORMATION SERVICES?

External information system services are services that are implemented outside of the system's authorization boundary (i.e., services that are used by, but are not a part of, the organization's information systems) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of information system security. These challenges include, but are not limited to: (i) defining the types of external services provided to the organization; (ii) describing how the external services are protected in accordance with the security requirements of the organization; and (iii) obtaining the necessary assurances that the risk to the organization's operations and assets, and to individuals, arising from the use of the external services is at an acceptable level.[18]

8. HOW DOES THE CATEGORIZATION DECISION AFFECT EXTERNAL INFORMATION SERVICES?

Categorizing external information system services provides the necessary information to determine the security requirements that the service provider should meet and the evidence that they should provide to achieve assurance that the external services are operating at an acceptable security level. The level of control over an external information system is usually established by the terms and conditions of the

[15] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 13

[16] NIST SP 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004, pp. 9-10

[17] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, pp. 23-24

[18] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, pp. 11-12

contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed security control requirements for the provider) to very limited (e.g., using a contract or service-level agreement to obtain commodity services). In other cases, a level of trust is derived from other factors that convince the authorizing official that the requisite security controls have been employed and that a credible determination of control effectiveness exists in the external system.[19]

Authorizing officials should require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Depending on the nature of the service, it may simply be unwise for the organization to wholly trust the provider—not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service. Where a sufficient level of trust cannot be established in the external services or service providers, the organization employs compensating controls or usage restrictions or accepts the greater degree of risk to its operations, assets, and individuals.[20]

CATEGORIZATION FUNDAMENTALS

9. WHAT IS THE DIFFERENCE, IF ANY, BETWEEN A SECURITY CATEGORY AND A SECURITY IMPACT LEVEL?

A security category is the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations and assets, individuals, other organizations, or the Nation.[21] Both information types and information systems have security categories—each with three components (one for each security objective) with a value of *low*, *moderate*, or *high*. However, an information system also has a security impact level, which consists of a single component with the value of *low*, *moderate*, or *high*. The security impact level for an information system is determined by taking the maximum impact value of the system's security category.

In summary, an information type has a security category with three components, one for each security objective. An information system has a security category and a security impact level that is derived from that security category. While the system's security impact level is used to look up the corresponding security control baseline (low, moderate, or high) in NIST SP 800-53, the system's security category (e.g., the specific impact value for a security objective such as integrity or availability) is considered when adjusting the system's security controls as defined in NIST SP 800-53.

10. HOW IS THE SECURITY CATEGORY EXPRESSED?

The generalized format for expressing the security category, SC, of an information type is:

$\text{SC}_{\text{information type}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)},

[19] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, p. 12

[20] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, p. 13

[21] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 8

where the acceptable values for potential impact are *low*, *moderate*, *high*, or *not applicable*. The potential impact value of *not applicable* only applies to the security objective of confidentiality.[22] For example, a security category for an information type that processes routine administration (non-privacy-related) information can be denoted as:

SC$_{\text{administrative information}}$ = {(confidentiality, low), (integrity, low), (availability, low)}.

The generalized format for expressing the security category, SC, of an information system is similar:

SC$_{\text{information system}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)},

where the acceptable values for potential impact are *low*, *moderate*, or *high*. The potential impact values assigned to the respective security objective (confidentiality, integrity, and availability) are the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system. The value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system.[23] For example, an information system that processes some information with a potential impact from a loss of confidentiality at moderate, some information with a potential impact from a loss of integrity at moderate, and all the information with a potential impact from a loss of availability at low, the security category of the information system can be expressed as:

SC$_{\text{information system}}$ = {(confidentiality, moderate), (integrity, moderate), (availability, low)}.

11. WHAT INFORMATION IS NEEDED TO CATEGORIZE AN INFORMATION SYSTEM?

Prior to categorizing a system, the system boundary should be defined.[24] Based on the system boundary, all information types associated with the system can be identified. Information about the organization and its mission, as well as the system's operating environment, intended use, and connections with other systems may affect the final security impact level determined for the information system. For example, if a system is connected to another system with a higher security impact level, it may be necessary to categorize the system at that higher impact level.

12. WHAT IS AN INFORMATION SYSTEM BOUNDARY?

The information system boundary is a logical group of information resources (information and related resources such as personnel, equipment, funds, and information technology) that have the same function or mission objectives, reside in the same general operating environment, and are under the same direct management control.[25]

[22] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 3

[23] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 4

[24] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 29

[25] 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, p. 16-17

13. WHEN SHOULD THE INFORMATION SYSTEM BOUNDARY BE ESTABLISHED?

The information system boundary should be established in the initiation phase of the system development life cycle before the initial risk assessment is conducted, the information system is categorized, and the system security plan is developed.[26]

14. WHO ESTABLISHES THE INFORMATION SYSTEM BOUNDARY?

Authorizing officials and senior agency information security officers consult with prospective information owners/information system owners to establish information system boundaries. The process of establishing boundaries for the organization's information systems and determining the associated security authorization implications of those boundaries is an organizational activity that should include careful negotiation among all key participants.[27] After the information system boundary is established, the information owner/information system owner and supporting information system security officer are responsible for the overall procurement, development, integration, modification, operation, and maintenance of the information system.[28]

15. HOW IS THE INFORMATION SYSTEM BOUNDARY ESTABLISHED?

Establishing boundaries for an organization's information systems takes into account the organization's mission or business requirements, the technical considerations with respect to information security, the programmatic costs to the organization, and the boundaries' effects on authorizing the organization's information systems. In order to identify the information system boundary, the information owner/information system owner needs to determine if the information resources:[29]

- Are under the same direct management control;
- Have the same function or mission objective and essentially the same operating characteristics and security needs; and
- Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).

Boundaries that are unnecessarily expansive (i.e., they include too many system components) make the information system difficult to manage and the security authorization process extremely unwieldy and complex. Boundaries that are unnecessarily limited increase the number of security authorizations that must be conducted and inflate the total security costs for the organization.[30]

Security categories can play an important part in defining appropriate authorization boundaries by partitioning information systems according to impact levels and the importance of those systems in carrying out the organization's missions and business processes. The partitioning process facilitates the

[26] 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, p. 16

[27] 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, p. 17

[28] 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, p. 13

[29] NIST 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, p. 16-17

[30] 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, p. 16

cost-effective application of security controls to achieve adequate security commensurate with the potential adverse impacts that may arise through the respective information systems.[31]

16. WHAT ARE THE VARIOUS TYPES OF INFORMATION THAT GOVERNMENT INFORMATION SYSTEMS PROCESS?

Information systems usually process several types of information. NIST SP 800-60 divides information into two major categories—information associated with an organization’s mission-specific activities and information associated with the administrative, management, and support activities common to most organizations. Each category supports two business areas, based on OMB’s Business Reference Model (BRM).

Mission-based information types are, by definition, specific to individual organizations or groups of organizations and are the primary source for determining the security impact values and security objectives for mission-based information and information systems. The consequences or impact of unauthorized disclosure of information, breach of integrity, and denial of services are defined by the nature and beneficiary of the service being provided or supported.[32] The two business areas associated with the mission-based information types include the following:

- The ***services for citizens*** business area describes the mission and purpose of the United States government in terms of the services it provides both to and on behalf of the American citizen. It includes the delivery of citizen-focused, public, and collective goods and/or benefits as a service and/or obligation of the federal government to the benefit and protection of the nation’s general population. An example of the *services for citizens* business area is the disaster management line of business that involves the activities required to prepare for, mitigate, respond to, and repair the effects of all disasters, whether natural or manmade. The disaster management line of business includes four information types: (i) disaster monitoring and prediction; (ii) disaster preparedness and planning; (iii) disaster repair and restore; and (iv) emergency response.[33]

- The ***mode of delivery*** business area describes the mechanisms that the government uses to achieve the purpose of government, or its services for citizens. An example of the *mode of delivery* business area is the federal financial assistance line of business that provides earned and unearned financial or monetary-like benefits to individuals, groups, or corporations. There are four information types associated with the federal financial assistance line of business: (i) federal grants; (ii) direct transfers to individuals; (iii) subsidies, and (iv) tax credits.[34]

Much of an organization’s information and supporting information systems are not used to provide direct mission-based services but primarily to support the delivery of services or to manage resources.[35] The two business areas associated with the management and support information types include the following:

[31] 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, p. 17

[32] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 15

[33] OMB, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007, pp. 27-36

[34] OMB, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007, pp. 36-38

[35] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 16

- The ***support delivery of services*** business area provides the critical policy, programmatic, and managerial foundation to support federal government operations. An example of the *support delivery of services* business area is the regulatory development line of business that involves activities associated with developing regulations, policies, and guidance to implement laws. The regulatory development line of business includes four information types: (i) policy and guidance development; (ii) public comment tracking; (iii) regulatory creation; and (iv) rule publication.[36]

- The ***management of government resources*** business area refers to the support activities that enable the government to operate efficiently. An example of the *management of government resources* business area is the human resource management line of business that involves all activities associated with the recruitment and management of personnel. The human resources management line of business includes ten information types: (i) human resources strategy; (ii) staff acquisition; (iii) organization and position management; (iv) compensation management; (v) benefits management; (vi) employee performance management; (vii) employee relations; (viii) labor relations; (ix) separation management; and (x) human resources development.[37]

Each information system may process information that does not fall neatly into one of the information types included in NIST SP 800-60, Volume II.[38] Once a set of information types has been identified for an information system, it is prudent to review the actual information processed, stored, or transmitted to determine if additional types of information need to be identified for security impact assessment purposes.[39]

17. HOW IS PERSONALLY IDENTIFIABLE INFORMATION (PII) HANDLED DURING THE CATEGORIZATION PROCESS?

The E-Government Act of 2002 strengthened the privacy protection requirements of the *Privacy Act of 1974*. Under the terms of these public laws, federal government agencies have specific responsibilities regarding the collection, dissemination, or disclosure of information regarding individuals. "Information in identifiable form is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)"[40]

Since most privacy regulations focus on sharing or disclosing information, privacy considerations affect the confidentiality impact level. In establishing confidentiality impact levels for each information type, the organization must consider the consequences of unauthorized disclosure of privacy information with respect to violations of federal policy and law. The confidentiality impact value of personally identifiable information will generally be *moderate*. The system's categorization documentation should be reviewed

[36] OMB, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007, pp. 39-42

[37] OMB, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007, pp. 42-46

[38] See question 18 for guidance on assigning an impact level to information types not included in NIST SP 800-60.

[39] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 14

[40] E-Government Act (P.L. 107-347), December 2002

to ensure that the consequences of privacy violations have been adequately factored into the system's security impact determination.[41]

ORGANIZATIONAL SUPPORT FOR THE CATEGORIZATION PROCESS FAQS

18. WHAT IS THE ORGANIZATION'S ROLE IN CATEGORIZING INFORMATION SYSTEMS?

In order to effectively support information owners/information system owners with the categorization process, the organization needs to establish relationships with other organizational entities, develop organization-wide categorization guidance, prepare a supplement to NIST SP 800-60, lead the organization-wide categorization sessions, and designate a point of contact to provide advice throughout the categorization process.

The success of the Risk Management Framework is dependent upon the collaboration among the organization's many entities. Typically this is led by the organization's information security program office. This office reaches out to information owners/information system owners to provide them with the guidance and support they need to effectively and consistently categorize their information systems. The information security program office also collaborates with the organization's enterprise architecture group, the personnel conducting the Capital Planning and Investment Control (CPIC) process, the information technology operations organization, and others to categorize the organization's information systems.

The information security program office should prepare categorization guidance that supplements the guidance in NIST SP 800-60 and provides organization-specific procedures and documentation, approval, and reporting requirements. The guidance is distributed to all individuals involved in the categorization process. The information security program office should also consider offering 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.

While NIST SP 800-60, Volume II, provides a comprehensive list of information types that are consistent with the Federal Enterprise Architecture, organizations may also identify additional information types that are unique to their mission. These additional, organization-specific information types need to be 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.

Organizations should conduct security categorizations of their information systems as an organization-wide activity with the 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 system security officers, chief information officer, senior agency information security officer, authorizing officials, and officials executing or participating in the

[41] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 30

risk executive function)[42] to ensure that each information system receives the appropriate management oversight and reflects the needs of the organization as a whole.[43]

Working together, senior leaders can make informed decisions, provide adequate security, mitigate risks, and help ensure the organization's missions and business activities remain functional. The risk management process begins with the categorization process, which influences all the remaining steps in the Risk Management Framework. A mistake in the initial security categorization process can result in either an over specification or an under specification of the security controls for the organization's information systems.[44]

19. HOW DO ORGANIZATIONS ESTABLISH MISSION-BASED INFORMATION TYPES?

Organizations may need to establish mission-based information types. The approach to establishing mission-based information types begins by documenting the organization's mission and business areas. In the case of mission-based information, the information security program office, in coordination with management, technical operations personnel, enterprise architecture, and other stakeholders, compiles a comprehensive set of the organization's mission areas, lines of business, and applicable sub-functions related to the lines of business and mission areas. For example, one organization's mission might be related to economic development. Sub-functions that are part of the organization's economic development mission might include business and industry development, intellectual property protection, or financial sector oversight. Each of these sub-functions represents an information type.[45]

When an organizational information type is not categorized in NIST SP 800-60, the responsible individuals within the organization must make an initial impact determination based on the FIPS 199 categorization criteria defined in Table 1, *Potential Impact Definitions for Security Objectives*.[46] For each information type, each security objective (confidentiality, integrity, and availability) is assigned an impact value (low, moderate, or high) by selecting and adjusting appropriate FIPS 199 Table 1 values.[47]

After the organization's information types have been identified, validated as consistent with the organization's enterprise architecture, and documented, the information security program office prepares a supplement to NIST SP 800-60 of additional, organization-specific information types, the recommended impact values for each security objective (confidentiality, integrity, and availability), the rationale for each impact value chosen, and the special factors affecting the impact determination for each organization-specific information type. The organization's supplement to NIST SP 800-60 should be distributed to information owner/information system owners for their use when categorizing their individual information systems.

[42] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 29

[43] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 29

[44] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 29

[45] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 16

[46] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 6

[47] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 19

20. How does the information system categorization affect the use of common security controls?

Common security controls are, in most cases, managed by an organizational entity other than the information owner/information system owner.[48] The common security controls are usually implemented by an organization or at a specific site and used to support multiple information systems (with various security categories) and organizational needs. The impact level associated with the organization's common controls should support the highest impact level of any individual information system within the organization relying on those common controls.[49]

The identification of common security controls is most effectively accomplished as an organization-wide exercise with the involvement of the chief information officer, senior agency information security officer, authorizing officials, information owner/information system owner, program managers, and information system security officers. The organization-wide exercise considers the categories of the information systems within the organization and the minimum security controls necessary to protect the operations and assets supported by those systems. The senior agency information security officer, acting on behalf of the chief information officer, coordinates with the common control provider that is responsible for the development and implementation of the designated common security controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information owner/information system owners to better support the security authorization process.[50]

If the organization chooses to implement common controls at an impact level that falls below the highest level required for individual information systems, the information owner/information system owners and authorizing officials for those systems should take appropriate actions to supplement those controls as required for any protection deficits that result at the system level.

System-specific Application of the Categorization Process FAQs

21. What are the steps to categorize an information system?

To categorize an information system, the information owner/information system owner identifies the information types, select the provisional impact value (low, moderate, or high) for each security objective (confidentiality, integrity, and availability) for each information type, adjust the provisional impact values for each information type, and assign the final security impact level for each information system.

Prepare for Categorization

In order to determine the system security category, the information owner/information system owner should collect relevant documentation specific to the information system such as the system description and architecture. In addition, the information owner/information system owner should also collect any available guidance documentation issued by the organization. The information owner/information system

[48] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 31

[49] NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008, p. 19

[50] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, pp. 10-11

owner should develop relationships with others within their organization that support the categorization process such as the information security program office, the enterprise architecture group, information sharing partners, and technical operations personnel.

Identify Information Types

The information owner/information system owner should determine the types of information that are processed by, stored in, or transmitted by the information system and document them in the system security plan. While most information types will be included in NIST SP 800-60, Volume II, or the organization's supplement to NIST SP 800-60, an information owner/information system owner may identify an information type unique to their information system.[51] If so, the unique information type should be documented and submitted to the organization's information security program office for validation and inclusion in the organization's supplement to NIST SP 800-60.

Select the Provisional Impact Values for Each Information Type

The information owner/information system owner should review NIST SP 800-60, Volume II, and the organization's supplement to NIST SP 800-60 and select the provisional, or initial, security category established for each information type.[52] The provisional security category of each information type should be documented in the system security plan. [See question 22 for guidance on the potential security impact values.]

Adjust the Information Type's Provisional Impact Values

The information owner/information system owner should review the appropriateness of the provisional impact values (low, moderate, high) for each security objective (confidentiality, integrity, and availability) for each information type in the information system based on the system's operational environment, mission, use, and connectivity with other systems. The provisional impact values should be adjusted as necessary based on the special factor guidance provided for each information type in NIST SP 800-60, Volume II,[53] or the organization's supplement to NIST SP 800-60. The rationale for adjusting the provisional impact value of each information type should be documented in the system security plan.

After the information types have been adjusted and documented in the system security plan, the information owner/information system owner should derive the provisional security category for the system by determining the highest value among each security objective (confidentiality, integrity, and availability) for the system's information types—that is, the highest impact value for confidentiality, the highest impact value for integrity, and the highest impact value for availability. [See question 23 for guidance on modifying the initial categorization of the system's information types.]

Adjust the Information Type's Security Category

After each information type has been adjusted and the provisional system security category has been determined, the information owner, with input from senior management, should review the impact values for confidentiality, integrity, and availability to determine if they are applicable to the information system or if a more realistic view of the potential impact on the system requires an increase in one or more

[51] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 19

[52] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 19

[53] NIST SP 800-60, Revision 1, *Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories, Volume II*, August 2008, pp. 7-101 and 107-231

security objectives of the system security category.[54] If the impact value for a security objective is changed, the final, adjusted system security category should be documented in the system security plan along with the rationale for the change. [See question 24 for guidance on adjusting the system's security category.]

Determine the System Security Impact Level

The information owner/information system owner assigns the one-value security impact level of *low*, *moderate*, or *high* to the information system.[55] For example, if the information system's security category is:

$SC_{\text{information system}}$ = {(confidentiality, HIGH), (integrity, MODERATE), (availability, LOW)},

the system security impact level is *high* since the impact value for the confidentiality security objective is *high*. The one-value, impact level is used to determine the initial security baseline during the select process while the system security category (three values, one for each security objective) is used to tailor the initial security control baseline.

The information system's impact level is documented in the system security plan. [See questions 25-27 for guidance on determining and documenting the system's security impact level.]

Obtain Approval for the System Security Category and Impact Level

The security category and impact level for the information system should be approved as defined in an organization's categorization guidance before continuing to the next step (Select) in the Risk Management Framework. It is important to validate the categorization decision since this decision determines the selection of security controls that are implemented in the information system.

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 the information processed, stored, or transmitted by the system to ensure that the system continues to support the organization's mission or business case. Changes to the information system or its operational environment may provide new insights as to the overall importance of the system in allowing the organization to fulfill its mission responsibilities.[56] [See question 28 for an example of modifying the security category and impact level.]

22. WHAT ARE THE POTENTIAL SECURITY 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) that represents a worst case scenario. The application of these definitions must take place within the context of each organization and the overall national interest. The potential impact is:[57]

[54] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 5

[55] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, p. 17

[56] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, p. 24

[57] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, pp. 2-3

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

Establishing an appropriate security category of an information type essentially requires determining the potential impact for each security objective associated with the particular information type. An additional impact value of *not applicable* only applies to the security objective of confidentiality if the information type is public information.[58]

23. HOW ARE THE SECURITY CATEGORIES OF INFORMATION TYPES ADJUSTED?

After each information type has been identified, the provisional security impact values[59] (*low*, *moderate*, *high*, or, for confidentiality only, *not applicable*[60]) are selected from the recommended provisional levels in NIST SP 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories* or the organization's supplement to NIST SP 800-60. The organization reviews the appropriateness of the provisional security impact values in the context of the organization and its mission as well as the system's operating environment, intended use, and connections with other systems.

NIST SP 800-60, Volume I, provides the criteria for adjusting the provisional security impact values. The confidentiality, integrity, and availability impact values may be adjusted as necessary during the review. [61] The special factor guidance in NIST SP 800-60, Volume II, provides guidance to adjust each information type. If the special factor guidance applies to the individual information system, the impact value for the security objective can be modified. For example, the Budget and Performance Integration Information Type includes the following special factor guidance for the confidentiality security objective that has a recommended impact value of *low*:

> In aggregate, budget and performance integration information can reveal capabilities and methods that some agencies (e.g., law enforcement, homeland security, national defense, intelligence) consider extremely sensitive. In these cases, the potential harm that can result from unauthorized disclosure ranges from *moderate* to *high* to *national security-related*.[62]

[58] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, p. 3

[59] The *provisional impact level* is the initial impact level assigned to the information type.

[60] The impact value for the *confidentiality* security objective can be *not applicable* if the information type is public information.

[61] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I,* August 2008, p. 23

[62] NIST SP 800-60, Revision 1, *Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories, Volume II,* August 2008, p. 24

In another example, the Contingency Planning Information Type has a recommended confidentiality impact value of *moderate*, but provides the following special factors guidance that allows a decrease of the recommended value:

> The consequences of unauthorized disclosure of extracts from contingency plans are likely to have negligible to limited adverse effects on agency operations. In such cases, the confidentiality impact would be, at most *low*.[63]

In addition, each information type should be evaluated with respect to the answers to questions such as the following:

- How can a malicious adversary use the information to do [limited, serious, severe] harm to organizational operations, organizational assets, or individuals?
- Would authorized disclosure or dissemination of elements of the information type violate laws, Executive Orders, or organizational regulations?
- What is the impact associated with unauthorized modification or destruction of the information or each unauthorized use of the information by the system?
- What is the impact associated with the loss of availability of the information in the system?

24. CAN THE SYSTEM’S SECURITY CATEGORY BE ADJUSTED?

Yes, in some cases the security category for a system may be higher than any impact value for any information type processed by the system. The following factors can be used to adjust the system security category above that of its constituent information types to reflect a more realistic view of the potential impact a security breach could have on the information system.

Aggregation

Some information may have little or no sensitivity in isolation but may be highly sensitive in aggregate. In some cases, the aggregation of large quantities of a single information type can reveal sensitive patterns or plans or facilitate access to sensitive or critical systems. In other cases, the aggregation of information of several different and seemingly innocuous types can have similar effects. If a review reveals increased sensitivity or criticality associated with information aggregates, an impact value for a security objective in the security category may need to be adjusted to a higher value than would be indicated by the impact values associated with any individual information type.[64]

Critical System Functionality

Compromise of some information types may have a low security impact value in the context of a system’s primary function but may have much more significance when viewed in the context of the potential impact on other systems to which the system is connected or on other systems that are dependent on that system’s information.[65]

[63] NIST SP 800-60, Revision 1, *Appendixes to Guide for Mapping Types of Information and Information Systems to Security Categories, Volume II,* August 2008, p. 27

[64] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I,* August 2008, p. 27

[65] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I,* August 2008, p. 27

Extenuating Circumstances

There are times when a system's security category should be elevated based on reasons other than its information. For example, the information system's critical process flow or security capability, the visibility of the system to the public, the sheer number of other systems reliant on its operation, or possibly its overall cost of replacement. These examples, given a specific situation, may provide reason for the information owner/information system owner to increase the impact value for one or more of the security objectives in the security category. An elevation of the security category based on extenuating circumstances can be more apparent by comparing the original security category to the business impact analysis.[66]

Public Information

Most organizations maintain web pages that are accessible to the public. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the organization. In most cases, the damage can be corrected within a relatively short period of time and the damage is limited (i.e., the impact value for integrity is *low*). In other cases (e.g., very large fraudulent transactions or modification of a highly visible web page), the damage to mission function or public confidence in the organization can be serious. In such cases, the integrity impact value associated with unauthorized modification or destruction of a public web page would be at least *moderate*.[67]

Catastrophic Loss of System Availability

Either physical or logical destruction of major assets can result in very large expenditures to restore the assets or result in long time periods for recovery. Permanent loss or unavailability of information system capabilities can seriously hamper an organization's operations, and, where direct services to the public are involved, have a severe adverse impact on public confidence in the organization. In the case of large systems, the loss of system availability may result in a high availability impact that is dependent on the cost and criticality attributes of the system rather than on the availability impact values of the types of information being processed by the system.[68]

Critical Infrastructures and Key National Assets

The *Critical Information Infrastructure Act of 2002* defines the term *critical infrastructure information* to mean "information not customarily in the public domain and related to the security of critical infrastructure or protected systems." If information types are aligned with critical infrastructures, then the information system must comply with Homeland Security Presidential Directive No. 7, *Critical Infrastructure Identification, Prioritization, and Protection.*[69] Where the mission served by an information system or the information that the system processes affects the security of critical national infrastructures or key national assets, the harm that results from a compromise requires particularly close

[66] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 28

[67] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 28

[68] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 28

[69] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 29

attention. The security category should be carefully determined when a loss of confidentiality, integrity, or availability will result in a negative impact of the critical infrastructure components and assets.[70]

Trade Secrets

There are several laws that specifically prohibit unauthorized disclosure of trade secrets. Therefore, if a system stores, communicates, or processes trade secrets, the information system's confidentiality security objective should be at least *moderate*.[71]

25. HOW IS THE OVERALL SECURITY IMPACT LEVEL OF THE INFORMATION SYSTEM DETERMINED?

The security impact level of a system will be the highest impact value for the security objectives (confidentiality, integrity, and availability) associated with the aggregate impact values of the system's information types (i.e., the system's security category). Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept (highest value) representing the worst case scenario is used to determine the security impact level of the information system.[72]

Therefore, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high-impact system is an information system in which at least one security objective is high.[73] The information system's impact level is subsequently used to select the initial set of baseline security controls from NIST SP 800-53. The end result produces an organization-wide view of the criticality and sensitivity of the information systems supporting mission/business processes and potential (worst case) impact to organizational operations and assets, individuals, other organizations, and the Nation should the information systems be compromised.[74]

26. SHOULD AN INFORMATION SYSTEM ALWAYS BE HIGH-IMPACT IF AT LEAST ONE OF ITS INFORMATION TYPES IS CATEGORIZED AS HIGH?

Yes, once the system security category has been determined (with impact values assigned to the respective security objectives), the system's impact level will be the highest value (high water mark) from among the values assigned to the security objectives in the security category. However, while the impact level is based on the high water mark and determines the initial security control baseline associated with the system (low, moderate, or high security baseline), organizations have the flexibility to adjust the

[70] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 29

[71] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 30

[72] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, p. 17

[73] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, p. 17

[74] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008, p. 29

security control baselines by following the scoping guidance, using compensating controls, and specifying organization-defined parameters as defined in NIST SP 800-53.[75]

27. HOW SHOULD THE INFORMATION SYSTEM CATEGORIZATION BE DOCUMENTED?

The information owner/information system owner must document the system categorization in the system security plan. In addition to the final categorization decision (i.e., the system's security impact level), the research, key decisions, and supporting categorization rationale should also be documented in the system security plan.

For each information type, the following information should be documented:

- The information type title;
- The reference to the catalog in which the information type is described (e.g., NIST SP 800-60, Volume II or the organization's supplement to NIST SP 800-60);
- The provisional security category of the information type; and
- If the provisional security category of the information type was changed:
  - The adjusted security impact values of the information type; and
  - Rationale for increasing or decreasing the impact value of the information type.

For the information system, the following information should be documented:

- The provisional (three-value) security category of the information system; and
- The (one-value) security impact level of the system (derived from the security category).

28. IS IT EVER NECESSARY TO MODIFY THE SECURITY CATEGORY OF AN INFORMATION TYPE?

Yes, there are times when it is necessary to modify the security category of an information type after the initial categorization is completed. The security impact values for an information type may vary throughout the system's life cycle. For example, contract information that has a *moderate* confidentiality impact value during the life of the contract may have a *low* impact value when the contract is completed.[76] Legislation may also levy additional requirements on some types of information. Some of the statutory and regulatory specifications are listed in NIST SP 800-60, Volume II.[77] The security category should be reviewed on an ongoing basis to help ensure that it reflect the current organizational environment and priorities.

[75] NIST SP 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, December 2007, pp. 17-18

[76] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 23

[77] NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I*, August 2008, p. 24