NIST RMF Quick Start Guide
CATEGORIZE STEP
Frequently Asked Questions (FAQs)

NIST Risk Management Framework (RMF) Categorize Step

Security categorization standards for information and systems provide a common framework and understanding for expressing security impacts that promotes: (i) effective risk management and oversight of 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 Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* [FIPS 199], and NIST SP 800-60, *Guide for Mapping Types of Information and Systems to Security Categories* [SP 800-60v1]. NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* [SP 800-122], provides guidance on how to assess confidentiality impacts for PII.

Contents

General Categorize Step FAQs 2

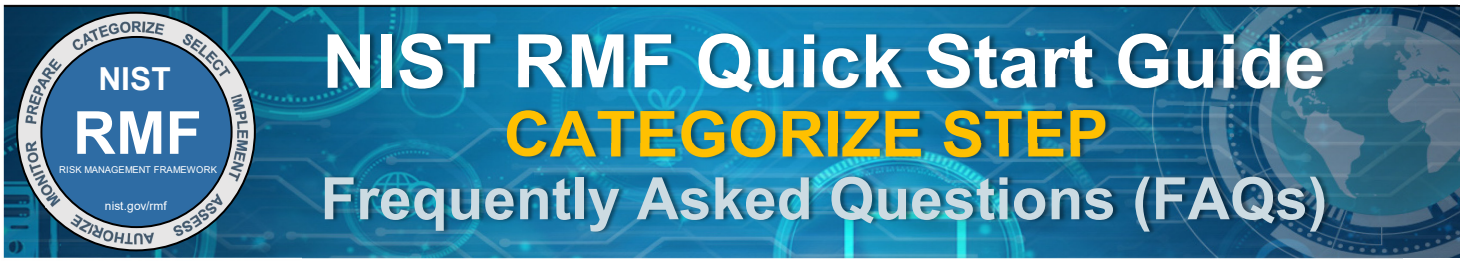
1. What has been modified from NIST SP 800-37, Rev. 1, to NIST SP 800-37, Rev. 2, for the Categorize step? 2
2. What is security categorization and why is it important? 3
3. How is the categorization decision used? 3
4. Who is responsible for categorizing each system? 3
5. What is the role of privacy in the categorization process? 4
6. What is the relationship between categorization and the organization's enterprise architecture? 4
7. What is the role of the risk executive (function) in the categorization process? 4
8. During which phase of the system development life cycle is a new system categorized? 4
9. How does the use of external system services impact system categorization? 5
10. How does the categorization decision affect external system services? 5

Categorize Step Fundamentals FAQs 6

11. What is the difference between a *security category* and a *security impact level*? 6
12. How is the security category expressed? 7
13. What information is needed to categorize a system? 7
14. How is the Categorize step related to FIPS publication 199? 7

Organizational Support for the Categorize Step FAQs 8

15. What is the organization's role in categorizing systems? 8
16. How does the system categorization affect the use of common controls? 9



System-specific Application of the Categorize Step FAQs 9
17. What are the steps to categorize a system? 9
18. What are the potential security impact values? 11
19. How are the security categories of information types adjusted? 11
20. Can the system's security category be adjusted? 12
21. How is the overall security impact level of the system determined? 13
22. Should a system always be high-impact if at least one of its information types is categorized as high? 14
23. How should the system categorization be documented? 14
24. Is it ever necessary to modify the security category of an information type? 14
25. What system characteristics does an organization document? 15
References 16

General Categorize Step FAQs

1. What has been modified from NIST SP 800-37, Rev. 1, to NIST SP 800-37, Rev. 2, for the Categorize step?

The following modifications have been made from NIST SP 800-37, Revision 1 [SP 800-37r1], to NIST SP 800-37, Revision 2 [SP 800-37r2], in the Categorize step:

- The *System Registration* task was moved to the Prepare step (Task P-18) to allow organizations to announce the existence of the system to the organization, add the system to the organizational system inventory, and explicitly announce implications to the organization's security and privacy programs from the creation of the system.
- The *Security Categorization Review and Approval* (Task C-2) task was added to ensure that the authorizing official reviews and approves the security categorization results to confirm that the security category selected for the system is consistent with the mission and business functions of the organization and the need to adequately protect those missions and functions.
- Elements of privacy and roles for systems that process personally identifiable information were added to this publication as a direct response to OMB Circular A-130 [OMB A130], which requires agencies to implement the Risk Management Framework (RMF) and integrate privacy into the RMF process. In establishing requirements for information security programs and privacy programs, the OMB Circular emphasizes the need for both programs to collaborate on shared objectives. [Back to Table of Contents]

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

Security categorization provides a structured way to determine the criticality of the information being processed, stored, and transmitted by a system. The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact of the loss of confidentiality, integrity, and availability of organizational systems and information to the organization. The categorization determination results in the security category for the system, which is based on the potential adverse impact (worst case) to an organization should events occur that jeopardize the information and 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. Before a security categorization decision can be made, the identification of the types of information that are or will be processed, stored, and transmitted by the system needs to be performed in the Prepare step (Task P-12, *Information Types*). Similarly, in addition to identifying the information types, each stage in the information life cycle for each type identified also needs to be identified and understood. This is also addressed in the Prepare step (Task P-13, *Information Life Cycle*).

The information owner or system owner identifies the types of information processed, stored, and transmitted by the system as part of Prepare step Task P-12 and assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type as part of Categorize step Task C-2. The high watermark concept is used to determine the security impact level of the system for the express purpose of prioritizing information security efforts among systems and selecting an initial set of controls from one of the three control baselines in NIST SP 800-53B [SP 800-53B]. According to the Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization for Federal Information and Information Systems* [FIPS 199], security categorization promotes effective management and oversight of information security programs, including the coordination of information security efforts across the Federal Government, and reporting on the adequacy and effectiveness of information security policies, procedures, and practices. [Back to Table of Contents]

3. How is the categorization decision used?

The categorization decision is used to support the next step in the Risk Management Framework: the Select step. It informs all subsequent risk management decisions regarding the security of the system. This includes baseline and control selection and documentation level of effort, implementation details, assessment level of effort, authorization decisions, continuous monitoring frequencies and level of effort, checks and balances for the initial risk assessment, and ongoing risk assessment. Once the overall security impact level of the system is determined (i.e., after the system is categorized), an initial set of controls is selected from the corresponding low, moderate, or high baselines in NIST SP 800-53B [SP 800-53B]. Organizations have the flexibility to adjust the control baselines following the tailoring guidance defined in NIST SP 800-53B [SP 800-53B] (i.e., applying scoping guidance, using compensating controls, specifying organization-defined parameters, and using supplemental controls). The security category and system security impact level are also used to determine the level of detail to include in security documentation, such as plans, procedures, and the level of effort needed to assess the system. [Back to Table of Contents]

4. Who is responsible for categorizing each system?

Ultimately, the information owner/system owner or an individual designated by the owner is responsible for categorizing a system. The information owner/system owner identifies all the information types stored in, processed by, or transmitted by the system as part of Prepare step Task P-12 and then determines the security category for the system by identifying the highest value (i.e., high water mark) for each security objective (confidentiality, integrity, and availability) and for each type of information resident on the system as part of Categorize step Task C-2. Subject matter experts may also be tapped by the information owner/system owner to assist with the system security categorization efforts. For systems that process personally identifiable information, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.

While the *primary* responsibility for categorization belongs to information owner/system owner, security categorizations are conducted as an organization-wide activity with the involvement of senior leadership (e.g., risk executive [function]) and system staff

(e.g., system security officer and system privacy officer when PII is being processed). The authorizing official or designated representative reviews the categorization results and decisions from other organizational systems and then collaborates with senior leaders to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high-value assets. Senior leadership participation 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. The authorizing official or designated representative reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with categorization decisions for all other organizational systems. [Back to Table of Contents]

5. What is the role of privacy in the categorization process?

Privacy programs are responsible for managing the risks to individuals associated with the processing of personally identifiable information (PII) and for ensuring compliance with applicable privacy requirements. When a system processes PII, the information security program and the privacy program have a shared responsibility for managing the security risks for the PII in the system. Informed by the privacy risk assessment conducted under the Prepare step (Task P-14, *Risk Assessment – System*), the privacy program and the security program collaborate on determining the security category and overall security impact level for the system. The senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.

6. What is the relationship between categorization and the organization's enterprise architecture?

The information types enumerated in NIST SP 800-60, Volume II [SP 800-60v2], are based on OMB's Business Reference Model (BRM) [OMB BRM], as described in the *Federal Enterprise Architecture Consolidated Reference Model Document*. The BRM provides a framework that facilitates 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. [Back to Table of Contents]

7. What is the role of the risk executive (function) in the categorization process?

The risk executive (function) may not necessarily be the responsibility of a single person. It could be the responsibility of a group, committee, or any entity as defined by the organization. This function helps ensure that information security considerations for individual 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 and business processes.

During the categorization process, the risk executive (function) provides the senior leadership with input and oversight to help ensure that consistent categorization decisions are made for individual systems across the organization. The risk executive (function) facilitates the sharing of security-related and risk-related information among senior leaders to help ensure that all types of risk that may affect mission and business success and the overall interests of the organization at large are considered. [Back to Table of Contents]

8. During which phase of the system development life cycle is a new system categorized?

The initial security categorization for the information and the system is performed during the initiation phase of the system development life cycle along with an initial security risk assessment. The initial risk assessment defines the threat environment in which the system operates and includes an initial description of the basic security needs of the system. These needs are contingent upon an understanding of how a possible loss of confidentiality, integrity, or availability of information of a system component can impact the organization and the resulting security categorization. For more details on security categorization, see Federal Information

Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems.* [FIPS 199]

Once the system is operational, the organization revisits the risk management activities described in the Risk Management Framework, including the system categorization, on a regular basis. Additionally, events can trigger an immediate need to assess the security state of the system. If a security event occurs, the organization may reexamine the security category and impact level of the system to confirm the criticality 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. [Back to Table of Contents]

9. How does the use of external system services impact system categorization?

The security categorization process assists a system or organization in assessing the impact of the loss of information confidentiality, integrity, or availability and helps define the necessary protection (controls) to reduce the likelihood of such losses. The organization then proceeds to the subsequent steps in the RMF until the system is authorized and continuously monitored. However, when using external system services (i.e., services that are implemented outside of the system's authorization boundary and are not part of the organization's systems), the organization typically has no direct control over the application of required controls or the assessment of 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 system security. These challenges include (i) defining the types of external services provided to the organization, (ii) describing how the external services are protected in accordance with the security and privacy 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. For example, the security categorization of cloud-based services that are identified and provided as part of their Federal Risk and Authorization Management Program (FedRAMP) [FedRAMP] authorization is reviewed along with the potential impacts, if any, to the organization utilizing these external system services. [Back to Table of Contents]

10. How does the categorization decision affect external system services?

Categorizing external systems and the organizational information processed, stored, and transmitted by external system services provides the necessary information to determine the security and privacy requirements that the service provider is required to meet and the evidence that they are required to provide to achieve assurance that the external services are operating at an acceptable security level. For example, if a system is categorized as a high impact system, and if the external system is categorized as a moderate impact system, then the organization needs to understand what the security implications are regarding the utilization of the external system services/resources. Thus, the security categorization of the organization acquiring external system services may influence or determine requirements for utilizing such services.

The level of control over an external system is usually established by the terms and conditions of the 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 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 in the external system service is derived from other factors that convince the authorizing official that the requisite controls have been employed and that a credible determination of control effectiveness exists in the external system.

Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with 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. [Back to Table of Contents]

Categorize Step Fundamentals FAQs

11. What is the difference between a *security category* and a *security impact level*?

Security category is the characterization of information or a system based on an assessment of the potential impact to organizational operations and assets, individuals, other organizations, or the Nation should there be a loss in *confidentiality*, *integrity*, or *availability* (security objectives) of such information or system. Note that an information type has a security category with three components – one for each security objective (i.e., confidentiality, integrity, or availability).

Security impact level consists of a single component with the value of *low*, *moderate*, or *high*. The security impact level for a system is determined by taking the maximum impact value of the system's security category – that is, the highest level ("high watermark") of the three security objectives for each information type and security category.

Table 1 Key terms

Key Terms	
SECURITY OBJECTIVES	*Confidentiality, integrity, and availability (of information and systems)*
SECURITY CATEGORIES	*Low, moderate, high (for each of the security objectives)*
SECURITY IMPACT LEVEL	*Low, moderate, high*

For example, in Table 2 below (extracted from Table C-2, *Type-based Impacts for Federal Information and Information Systems*, in NIST SP 800-60, Volume 2, *Guide for Mapping Types of Information and Information Systems to Security Categories* [SP 800-60v2]), there is an information type ("C.3.5.8 System and Network Monitoring") with a Moderate confidentiality impact level, a Moderate integrity impact level, and a Low availability impact level:

Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)}[1]

Table 2 Sample security category

Security Categorization of Management and Support Information			
C.3.5 Information & Technology Management	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
C.3.5.8 System and Network Monitoring	Moderate	Moderate	Low

For illustration purposes, the security category for the information or system is Moderate (the high watermark between Moderate-Moderate-Low).

While the system's security impact level is used to look up the corresponding control baseline (low, moderate, or high) in NIST SP 800-53B [SP 800-53B], the system's security category (e.g., the specific impact value for each of the three security objectives:

[1] See *How is the security category expressed?* question and answer for expanded description.

confidentiality, integrity, and availability) is considered when adjusting the system's controls, as defined in NIST SP 800-53 [SP 800-53r5]. [Back to Table of Contents]

12. How is the security category expressed?

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

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

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. For example, a security category for an information type that processes routine administrative information (non-PII) can be denoted as:

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

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

$$SC_{\text{system}} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\},$$

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 system. The value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for a system. For example, a 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, may have a security category expressed as:

$$SC_{\text{system}} = \{(\text{confidentiality, moderate}), (\text{integrity, moderate}), (\text{availability, low})\}$$ [Back to Table of Contents]

13. What information is needed to categorize a system?

Information needed to categorize a system is now being collected in the Prepare step of the Risk Management Framework. Prior to categorizing a system, the authorization boundary needs to be defined. This is now done by task P-11, *Authorization Boundary*, per SP 800-37, Revision 2 [SP 800-37r2]. Based on the authorization boundary, all information types associated with the system can be identified. The identification of information types and information life cycle is now done by tasks P-12, *Information Types*, and P-13, *Information Life Cycle*, in NIST SP 800-37, Revision 2. 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 system. [Back to Table of Contents]

14. How is the Categorize step related to FIPS publication 199?

FIPS Publication 199 defines the security categorization standard and provides guidance along with NIST SP 800-60, *Guide for Mapping Types of Information and Systems to Security Categories* [SP 800-60v1]. In accordance with FIPS Publication 199, agencies shall identify all of the applicable information types that are representative of input, stored, processed, and/or output data from each system. The initial activity in mapping types of federal information and systems to security objectives and impact levels is the development of an information taxonomy or the creation of a catalog of information types. The basis for the identification of information types is the OMB's Business Reference Model (BRM) [OMB BRM] Federal Enterprise Architecture (FEA) [OMB FEA] Consolidated Reference Model Document. Each category supports two business areas based on OMB's Business Reference Model (BRM). [Back to Table of Contents]

Organizational Support for the Categorize Step FAQs

15. What is the organization's role in categorizing systems?

In order to effectively support information owners and 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, Volume I [SP 800-60v1]; lead 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 collaboration among the organization's many entities. Typically, this is led by the organization's information security program office. The information security program office reaches out to the information owner/system owner to provide them with the guidance and support they need to effectively and consistently categorize their systems. The information security program office also collaborates with the organization's enterprise architecture group, the personnel conducting the capital planning and investment control process, the information technology operations organization, and others to categorize the organization's systems.

The information security program office prepares categorization guidance that supplements the guidance in NIST SP 800-60 and provides organization-specific procedures, documentation, approval, and reporting requirements. The guidance is distributed to all individuals involved in the categorization process. The information security program office also considers offering training to individuals involved in the categorization process. Training ensures that the organization-specific guidance, tools, templates, and techniques are applied consistently throughout the organization.

While NIST SP 800-60, Volume II [SP 800-60v2], provides a comprehensive list of information types that are consistent with the Federal Enterprise Architecture [OMB FEA], organizations may also identify additional information types that are unique to their mission (e.g., National Archives and Records Administration Controlled Unclassified Information Registry [NARA CUI]). The 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 owner/system owner for use in their system categorization efforts.

Organizations conduct security categorizations of their 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 owner/system owner, enterprise architects, information technology planners, system security officers, chief information officer, senior agency information security officer, authorizing officials, and officials executing or participating in the risk executive function) to ensure that each system receives the appropriate management oversight and reflects the needs of the organization as a whole.

The authorizing official or designated representatives reviews the categorization results and decision from an organization-wide perspective, including how the decision aligns with categorization decisions for all other organizational systems. The authorizing official collaborates with the senior agency official for risk management or the risk executive (function) to ensure that the categorization decision for the system is consistent with the organizational risk management strategy and satisfies requirements for high-value assets.

Working together, senior leaders can make informed decisions, provide adequate security, mitigate risks, and help ensure the organization's mission 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 controls for the organization's systems. [Back to Table of Contents]

16. How does the system categorization affect the use of common controls?

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

The identification of common controls, which is part of Task P-5 in the Risk Management Framework, is most effectively accomplished as an organization-wide exercise with the involvement of the chief information officer, senior agency information security officer, senior agency official for privacy, authorizing officials, information owner/system owner, program managers, and system security and system privacy officers. The organization-wide exercise considers the categories of the systems within the organization and the minimum 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 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/system owner to better support the security authorization process.

If the organization chooses to implement common controls at an impact level that falls below the highest level required for individual systems, the information owner/system owner and authorizing officials for higher impact systems take appropriate actions to supplement the lower impact common controls, as required for any protection deficits that result at the system level. [Back to Table of Contents]

System-specific Application of the Categorize Step FAQs

17. What are the steps to categorize a system?

To categorize a system, the information owner/system owner identifies the information types (Task P-12 in the Prepare step of the Risk Management Framework), selects the provisional impact value (low, moderate, or high) for each security objective (confidentiality, integrity, and availability) and for each information type, adjusts the provisional impact values for each information type, and assigns the final security impact level for each system.

Prepare for Categorization

In order to determine the system security category, the information owner/system owner collects relevant artifacts specific to the system, such as the system description and architecture. In addition, the information owner/system owner also collects any available guidance artifacts issued by the organization. The information owner/system owner develops relationships with others within their organization who support the categorization process, such as the information security program office, the enterprise architecture group, information sharing partners, and technical operations personnel. *Note that many of these activities are addressed by system-level tasks of the Prepare step.*

Identify Information Types

The information owner/system owner determines the types of information that is processed by, stored in, or transmitted by the system and documents the information types in the security and privacy plans. This is Task P-12, *Information Types*, of the Prepare step. While most information types are included in NIST SP 800-60, Volume II [SP 800-60v2], or the organization's supplement to NIST SP 800-60, an information owner/system owner may identify an information type unique to their system. If so, the unique information type is 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. Note that once information types are identified, all stages of the information life cycle for each information type also needs to be identified and understood. This is addressed by Task P-13, *Information Life Cycle*.

Select the Provisional Impact Values for Each Information Type

The information owner/system owner reviews NIST SP 800-60, Volume II, and the organization's supplement to NIST SP 800-60 and selects the provisional or initial security category established for each information type. The provisional security category of each information type is documented in the security and privacy plans.

Adjust the Information Type's Provisional Impact Values

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

After the information types have been adjusted and documented in the security and privacy plans, the information owner/system owner derives 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 (i.e., the highest impact value for confidentiality, the highest impact value for integrity, and the highest impact value for availability).

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 – reviews the impact values for confidentiality, integrity, and availability to determine if they are applicable to the system or if a more realistic view of the potential impact on the system requires an increase in one or more security objectives of the system security category. If the impact value for a security objective is changed, the final, adjusted system security category is documented in the security and privacy plans along with the rationale for the change.

Determine the System Security Impact Level

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

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

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 control baseline.

The system impact level is documented in the security and privacy plans.

Obtain Approval for the System Security Category and Impact Level

The security category and impact level for the system is 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 the categorization decision determines the selection of controls that are implemented in the system. For information systems that process personally identifiable information, the senior agency official for privacy reviews and approves the security categorization results and decision prior to the authorizing official's review.

Maintain the System Security Category and Impact Level

Periodically the information owner/system owner reconfirms the criticality of the 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 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. [Back to Table of Contents]

18. What are the potential security impact values?

FIPS Publication 199 defines three levels of potential adverse 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 the impact level definitions takes place within the context of each organization and the overall national interest. The potential impacts are:

- ***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. [Back to Table of Contents]

19. How are the security categories of information types adjusted?

After each information type has been identified, the provisional security impact values (*low*, *moderate*, *high*, or, for confidentiality only, *not applicable*) are selected from the recommended provisional levels in NIST SP 800-60, Volume II: *Appendices to Guide for Mapping Types of Information and Systems to Security Categories* [SP 800-60v2], 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 [SP 800-60v1], 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. 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 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*.

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*.

In addition, each information type is 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 the 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? [Back to Table of Contents]

20. 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 that a security breach could have on the 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 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.

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.

Extenuating Circumstances

There are times when a system's security category is elevated based on reasons other than its information, such as the 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 the potential overall cost of replacement. These examples, given a specific situation, may provide reason for the information owner/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 made more apparent by comparing the original security category to the business impact analysis.

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 the destruction of a public web page would be at least moderate.

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 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.

Critical Infrastructures and Key National Assets

The Critical Information Infrastructure Act of 2002 [HSACT 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 system must comply with Homeland Security Presidential Directive No. 7, *Critical Infrastructure Identification, Prioritization, and Protection* [HSPD-7]. Where the mission served by a 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 attention. The security category is carefully determined when a loss of confidentiality, integrity, or availability results in a negative impact of the critical infrastructure components and high-value assets (HVAs)[2].

Trade Secrets

There are several laws that specifically prohibit the unauthorized disclosure of trade secrets. Therefore, if a system stores, communicates, or processes trade secrets, the system's confidentiality security objective is at least moderate. [Back to Table of Contents]

21. How is the overall security impact level of the system determined?

The security impact level of a system is 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 system, the high watermark concept (highest value) representing the worst-case scenario is used to determine the security impact level of the system.

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

[2] High-value assets do not necessarily impact the categorization. However, having HVAs in and/or interconnected with the authorization boundary may impact the categorization.

organizational operations and assets, individuals, other organizations, and the Nation should the systems be compromised. [Back to Table of Contents]

22. Should a 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 is 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 watermark and determines the initial security control baseline associated with the system (low, moderate, or high security baseline), organizations have the flexibility to adjust the control baselines by following the tailoring guidance as defined in NIST SP 800-53B [SP 800-53B] (i.e., applying scoping guidance, using compensating controls, specifying organization-defined parameters, and using supplemental controls). [Back to Table of Contents]

23. How should the system categorization be documented?

The information owner/system owner documents the system categorization in the security and privacy plans. In addition to the final categorization decision (i.e., the system's security impact level), the research, key decisions, and supporting categorization rationale are also documented in the security and privacy plans.

For each information type, the following information is documented:

- Information type title
- Reference to the catalog in which the information type is described (e.g., NIST SP 800-60, Volume II [SP 800-60v2], or the organization's supplement to NIST SP 800-60)
- Provisional security category of the information type
- 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 system, the following information is documented:

- Provisional (three-value) security category of the system
- The (one-value) security impact level of the system (derived from the security category) [Back to Table of Contents]

24. 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. 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 [SP 800-60v2]. The security category is reviewed on an ongoing basis to help ensure that it reflects the current organizational environment and priorities. [Back to Table of Contents]

25. What system characteristics does an organization document?

A description of the system characteristics is documented in the security and privacy plans, included in attachments to the plans, or referenced in other standard sources for the information generated as part of the system development life cycle. Duplication of information is avoided whenever possible. The level of detail in the security and privacy plans is determined by the organization and is commensurate with the security categorization and the security and privacy risk assessments of the system. Information may be added to the system description as it becomes available during the system life cycle and execution of the RMF steps.

System characteristics include:

- Descriptive name of the system,
- System version or release number,
- Purpose of the system,
- Incident response points of contact,
- Authorization date and authorization termination date, and
- Network topology and architecture description.

[Back to Table of Contents]

References

[FedRAMP] General Services Administration, *Federal Risk and Authorization Management Program* (FedRAMP) https://www.fedramp.gov

[FIPS 199] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[HSACT 2002] Homeland Security Act of 2002, Pub. L. 107-296 Stat 2135 https://www.govinfo.gov/app/details/COMPS-1143

[HSPD-7] Department of Homeland Security, *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (HSPD-7), June 27, 2008. Available at https://www.cisa.gov/homeland-security-presidential-directive-7

[NARA CUI] National Archives and Records Administration, *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui

[OMB A130] Office of Management and Budget (2016) *Managing Information as a Strategic Resource*. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[OMB BRM] Office of Management and Budget, *The Business Reference Model, Version 3.1 A Foundation for Government-wide Improvement.* May 2013. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/brm_v3-1-service_codes_and_definitions_rev1_20130615.pdf

[OMB FEA] Office of Management and Budget, *Federal Enterprise Architecture (FEA)*. January 2013. https://obamawhitehouse.archives.gov/omb/e-gov/fea

[SP 800-37r1] Joint Task Force (2010) Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 1 [withdrawn]. https://doi.org/10.6028/NIST.SP.800-37r1

[SP 800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-53r5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5

[SP 800-53B] Joint Task Force (2020) Control Baselines for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B

[SP 800-60v1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP 800-60v2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP 800-122] McCallister E, Grance T, Scarfone KA (2010) Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-122. https://doi.org/10.6028/NIST.SP.800-122

[Back to Table of Contents]