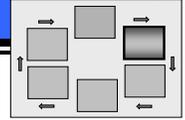


SELECT STEP – TIPS AND TECHNIQUES FOR SYSTEMS



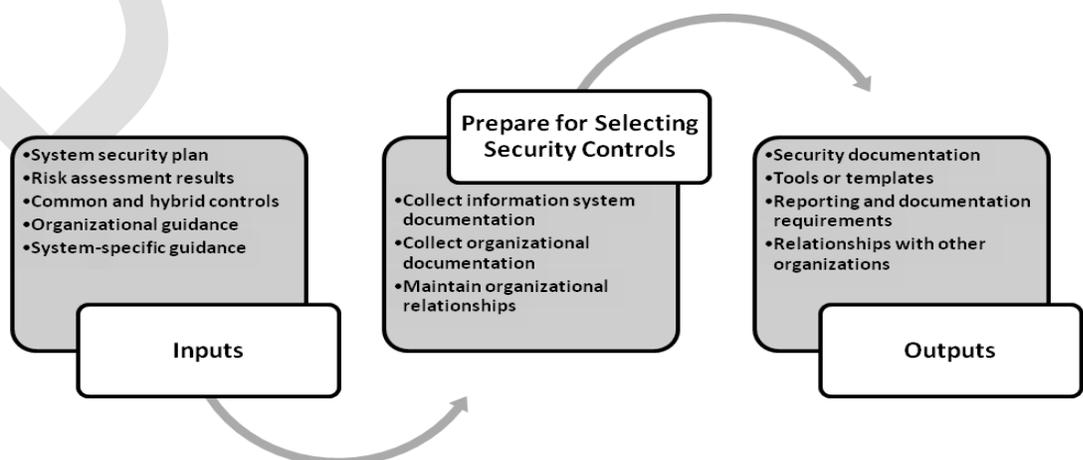
Selecting the appropriate security controls for the organization's information systems can have major implications on the operations and assets of an organization as well as the welfare of individuals and the Nation. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for federal information and information systems in seventeen security-related areas. All federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls defined in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, as amended. NIST SP 800-53 represents the current state-of-the-practice safeguards and countermeasures for information systems and is used to establish a level of due diligence in protecting the organization's information systems.

NOTE: The *Tips and Techniques for Systems* is provided as one approach of how to select security controls for information systems when implementing NIST SP 800-53. Readers should understand that other approaches may be used to support their particular circumstances. The tables are used to illustrate the approach and are not required.

NIST SP 800-53 identifies the process to select the appropriate set of security controls for an information system that consists of the following tasks: (i) choosing a set of baseline security controls; (ii) tailoring the baseline security controls by applying scoping guidance, parameterization, and compensating control guidance; (iii) supplementing the tailored baseline security controls, if necessary, with additional controls or control enhancements to address unique organizational needs based on a risk assessment (either formal or informal) and local cost-benefit analyses, or special circumstances; and (iv) specifying minimum assurance requirements, as appropriate.

PREPARE FOR SELECTING SECURITY CONTROLS

In order to select the appropriate security controls for the information system, the information system owner collects relevant documentation specific to the information system such as the initial system security plan and the risk assessment results. In addition, the information system owner also collects any available guidance documentation issued by the organization. The information system owner continues their relationships with others within the organization that are also impacted by the security control selection process (e.g., information security program office, information sharing partners, contracts/acquisition organization).



Collect Information System Documentation

Prior to selecting security controls for an information system, the information owner collects the initial system security plan, risk assessment results, and other available documentation on the information system. The initial security plan includes the results of the system categorization, system description and architecture, and interconnections with other systems. The risk assessment results include a summary of the potential threats to and vulnerabilities in the information system and the planned or in place mitigations against those threats and vulnerabilities. The risk assessment should be conducted consistent with NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*,¹ with the results documented in the system security plan or a separate risk assessment report. Security-related documents are developed throughout the system development life cycle.

Collect Organizational Documentation

Information owners also obtain organization-specific guidance on how to select, tailor, supplement, and document security controls for their information systems. Typically organizations have guidance that elaborates on the NIST standards and guidance and that provides organization-specific implementation details, including organization-specific tools, templates, or checklists to support the selection process. The organization-specific guidance usually includes internal requirements for reporting and approving the selected set of security controls for the information system.

Organizations also identify their common controls and the common portion of hybrid controls. The senior information security officer is responsible for coordinating with the common control provider (e.g., facilities managers, site managers, personnel managers) responsible for the development and implementation of the designated common controls to ensure that the controls are put into place, assessed, and the assessment results are shared with information system owners. The common and hybrid controls are published in a format that allows information system owners to gain the information necessary to incorporate the common controls and common portion of hybrid controls into their individual information systems.

Maintain Organizational Relationships

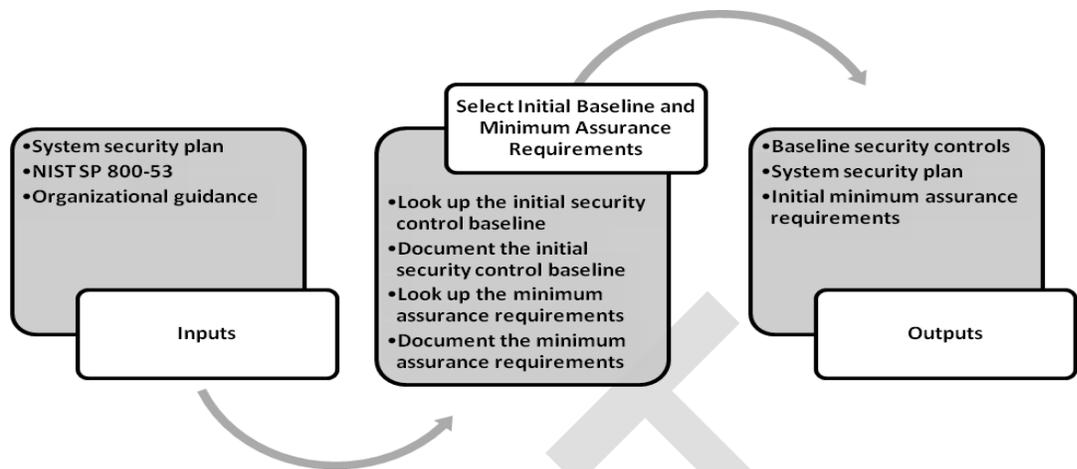
In addition to gathering documentation, information owners maintain relationships with others within their organization. The information security program office establishes the organization-specific policies on conducting a risk assessment, selecting security controls, and documenting the selection process in the security plan. The office may also provide tools, templates, or checklists to assist with the selection and documentation processes. The information security program office is the primary contact for advice and support while selecting the security controls for individual information systems.

The information owner also works with others within the organization including the enterprise architecture group, information sharing partners, and technical operations personnel. Each of these groups provides a portion of the information needed to effectively select the information system's security controls.

SELECT THE INITIAL SECURITY CONTROL BASELINE AND MINIMUM ASSURANCE REQUIREMENTS

Once the system's impact level is determined, the initial set of security controls and minimum assurance requirements are identified. The initial set of security controls is selected from the corresponding low, moderate, or high baselines listed in NIST SP 800-53, Appendix D. The minimum assurance requirements are defined in NIST SP 800-53, Appendix E. The minimum assurance requirements are grouped by system impact level and apply to each control within the final, selected set of security controls.

¹ The first public draft of NIST SP 800-30, Revision 1 is expected in early 2011 and will focus on risk assessment throughout the Risk Management Framework.



Look Up the Initial Security Control Baseline

The system’s security impact level, identified during the Categorize Step, determines the initial security baseline. Using the security impact level (low-, moderate-, or high-impact), choose the appropriate baseline listed in NIST SP 800-53, Appendix D. If a security control is not used in a particular baseline, the entry is marked as *not selected*. For example, a system with a moderate impact level would include all the security controls in the “MOD” column from NIST SP 800-53, Appendix D.

Some security controls, supplemental guidance for the controls, and control enhancements in the security control catalog are not used in any of the baselines but are available for use by organizations, if needed. A complete description of each security control, supplemental guidance for the control, and control enhancements is provided in NIST SP 800-53, Appendix F.

Document the Initial Security Control Baseline

The security controls can be listed in a spreadsheet or table similar to the one below (that can be expanded and updated throughout the selection process and used in later steps in the Risk Management Framework).² The spreadsheet/table provides a way to summarize the decisions made during the tailoring and supplementation processes that result in the selected set of security controls for the information system. The table can be included as an appendix to the system security plan, while detailed information on how each of the security controls is implemented is included in the main body of the security plan.

All the security controls in the selected baseline are listed in the appropriate column in the spreadsheet/table. The initial information that is recorded is the family identifier, control number, and control name. Control enhancements, when used to supplement basic security controls, are indicated by the number of the control enhancement in parentheses. During the tailoring process, additional information is added to the table.

NO.	CONTROL NAME	TAILORING	RATIONALE
AC-1	Access Control Policy and Procedure		
....			
AC-3	Account Enforcement		
....			
AT-3	Security Training		
AT-4	Security Training Records		
....			

² This table is an example used to illustrate an approach to recording the selection and supplementation of security controls and the rationale justifying the decision. It is not a mandatory format. Organizations may develop their own unique method to capture the information consistent with the requirements in NIST SPs 800-53 and 800-37.

CP-2	Contingency Plan		
CP-2(1)	Contingency Plan		
CP-3	Contingency Training		
....			
IA-3	Device Identification and Authentication		
IA-4	Identifier Management		
....			
PE-14	Temperature and Humidity Controls		
PE-15	Water Damage Protection		
....			
SC-12	Cryptographic Key Establishment and Management		
SC-13	Use of Cryptography		
....			
SI-11	Error Handling		
SI-12	Information Output Handling and Retention		

Look Up the Minimum Assurance Requirements

The minimum assurance requirements for an information system are defined in NIST SP 800-53, Appendix E. The assurance requirements are directed at the activities and actions that security control developers and implementers define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

The system’s impact level determines the appropriate minimum assurance requirements. Low-impact systems following the low baseline minimum assurance requirements, while moderate- and high-impact systems following the moderate or high baseline minimum assurance requirements.

Document the Minimum Assurance Requirements

The minimum assurance requirements are documented in the security plan. For example, a moderate-impact information system is expected to implement the moderate-impact minimum assurance requirements, recording the assurance requirements in the security plan in the general description section.³

Section X.Y Minimum Assurance Requirements

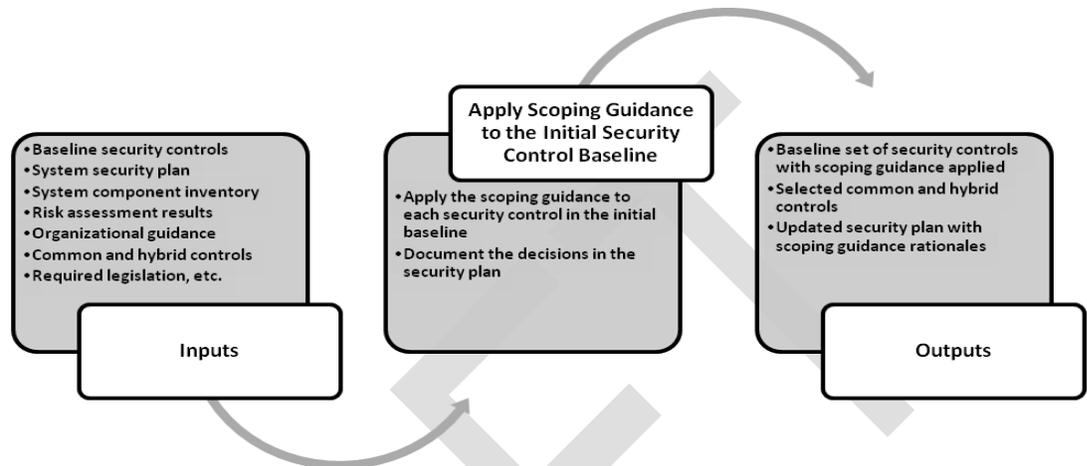
Moderate Impact Information Systems: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

APPLY SCOPING GUIDANCE

Organizations have the flexibility to tailor the security control baselines following the guidance in NIST SP 800-53. Tailoring activities include: (i) the application of appropriate scoping guidance to the initial baseline; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.

³ This sample shows one way that the minimum assurance requirements can be documented in the system security plan. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-37.

When applying scoping guidance, the information system owner reviews the information system to determine if the scoping guidance (e.g., use of common controls, physical infrastructure-related considerations, or technology-related considerations) is applicable to each security control in the information system. If the scoping guidance applies, the appropriate action (e.g., does not apply, downgraded) is noted in the spreadsheet/table used to document the security control selection process.



**Apply Operational/
Environmental-
related
Considerations**

Security controls that are dependent on the nature of the operational environment are applicable only if the information system is employed in an environment necessitating the controls. For example, temperature and humidity controls may not be applicable to remote sensors that exist outside of the indoor facilities where other information system components are located.

Review each security control and determine if the control does or does not apply to the information system or specific components within the information system based on the system's operational/environmental conditions. If the security control does not apply to the information system, mark the control in the spreadsheet/table as *does not apply* and explain the rationale justifying why the control does not apply. If the security control does not apply to specific components in the information system (e.g., remote sensors), identify the component to which the controls do not apply.

**Apply Technology-
related
Considerations**

Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system. In addition, the security controls apply only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.

The information system owner also determines if an automated mechanism that could explicitly or implicitly support a security control is readily available in COTS or GOTS products, is cost-effective, and technically feasible. If the automated mechanism is not readily available, cost-effective, or technically feasible, compensating security controls are implemented through non-automated mechanisms or procedures.

Review each security control and determine if the control does or does not apply to the information system or specific components within the information system based on the implemented technologies and available automated mechanisms. If the security control does not apply to the information system, mark the control in the spreadsheet/table as *does not apply* and explain the rationale justifying why the control does not apply. If the

security control applies only to selected components within the information system, identify the components to which the control applies.

Apply Physical Infrastructure-related Considerations

Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as email or web servers, server farms, data centers, networking nodes, boundary protection devices, and communications equipment).

Organizational facilities often implement security controls as common controls that apply to multiple information systems. If the physical infrastructure-related security control is implemented as a common control, mark the control in the spreadsheet/table as *common control* and identify the components to which the security controls apply.

The common control may not provide sufficient security protection to the information system. If any of the system components need system-specific infrastructure protections, in addition to common controls that apply to the information system, the control is implemented as a hybrid control. Mark the control in the spreadsheet/table as *hybrid control* and identify the components to which the security control applies. For example, emergency power may be implemented as a common control for the facility in which the system resides, but the specific information system requires additional availability protection based on the criticality of the information in the system to the organization's mission resulting in the implementation of a separate uninterrupted emergency power source for the information system.

Apply Public Access-related Considerations

Some information systems allow public access. Security controls associated with public access information systems are carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to users accessing information systems through public interfaces. The type of information accessed through the publically-available system is also carefully considered. If users are accessing public information through a public interface, access controls may not be necessary. On the other hand, access controls would be required for users accessing their personal information through a public interface or by organizational personnel that maintain and support the information system.

Review each security control and determine if the control does or does not apply to the information system or specific components within the information system based on the public access needs associated with the information system. If the security control does not apply to the information system, mark the control in the spreadsheet/table as *does not apply* and explain the rationale justifying why the control does not apply. If the security control applies only to specific system components or system users, identify the specific components related to the control in the spreadsheet/table.

Apply Policy/Regulatory-related Considerations

Security controls that address matters governed by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations. For example, OMB 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002. If the information in the system does not contain the types of information specified by the OMB regulation, the security control does not apply.

Review each security control and determine if the control does or does not apply to the information system or specific components within the information system based on the applicable laws, Executive Orders, directives, policies, standards, or regulations that apply

to the information system. If the security control does not apply to the information system, mark the control in the spreadsheet/table as *does not apply* and explain the rationale justifying why the control does not apply.

Apply Security Objective-related Considerations

Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the security category for the supported security objectives of confidentiality, integrity, or availability before moving to system's impact level (i.e., high water mark); (ii) is supported by an organizational assessment of risk; and (iii) does not adversely affect the level of protection for the security-relevant information within the information system.

Review each security control and determine if a security control that uniquely supports the confidentiality, integrity, or availability of the system may be available for downgrading (e.g., if the system's impact level is moderate based on the security category for confidentiality and integrity being moderate, while the security category for availability is low, controls uniquely related to availability may be downgraded to the low-impact baseline). NIST SP 800-53 identifies specific controls that are recommended candidates for downgrading. If the security control is downgraded to a control in a lower baseline, mark the control in the spreadsheet/table as *downgraded*.

If an impact value for a security objective in the security category is lower than the system's impact level (e.g., the impact value in the security category for availability is low, while the system's impact level is moderate), examine the corresponding security controls in the lower baseline and analyze the risks to the system if the security control in the lower baseline is used and whether and how the downgrading action affects the security-relevant information within the information system. If a corresponding security control in the lower baseline is not selected, analyze the risks to the systems if the security control that corresponds with the system's impact level is not used and whether and how the absence of the security control that corresponds with the system's impact level affects the security-relevant information within the system. Depending on the analysis, the security control could be eliminated or modified to accommodate the risks to the system.

If the security control is downgraded to a lower baseline or control enhancement, mark the control in the spreadsheet/table as *downgraded to security control number/enhancement* and explain the rationale. If the security control is modified to accommodate risks to the system, identify the modifications. If, based on a thorough analysis, the information system owner determines the elimination of the controls does not pose security risks to the information system, mark the control in the spreadsheet/table as *does not apply* and explain the rationale.

Apply Common Control-related Considerations

Some security controls or portions of security controls are implemented by the organization and apply to multiple information systems. These controls are known as common controls or hybrid controls. Individual information system owners do not need to implement and assess the common controls or the common portion of hybrid controls, but do need to identify if common or hybrid controls are applicable to the system and incorporate the assessment results into the information system's security plan either directly or by reference. Every control in a baseline must be fully addressed, either by the organization or the information system owner. The information security program office publishes the common and hybrid controls in a format that provides contact information for each control and the applicability of the control along with guidance on how to obtain the assessment results for the control.

Review each security control and determine if the organization has a common or hybrid control that is applicable to the information system or specific components within the information system. If there is a common or hybrid control that is applicable to the

information system, the information system owner determines if the common control or the common portion of the hybrid control is sufficient to meet the information system's requirements (e.g., does it provide sufficient protection against potential system risks).

If the security control can be implemented as a common control, mark the control in the spreadsheet/table as *common* and explain the rationale justifying why the control can be implemented as a common control. If only a portion of the control can be implemented as a common control, mark the control in the spreadsheet/table as *hybrid*, explain which portion of the control is common and which portion is system-specific, and justify why the control can be implemented as a hybrid control.

System Component Allocation-related Considerations

Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control. Review the inventory of information system components to determine which security controls are applicable to the various components and decide where to allocate the controls in order to satisfy organizational security requirements. Document the system components that are associated with each security control. For new system development, the system components associated with the security controls may not be known during the Select Step. The system's component allocation-related considerations may be refined during the Implement Step.

Apply Scalability-related Considerations

Scalability-related considerations apply to how the control is implemented and the documentation produced for the security control. Scalability is guided by the system's impact level, with more detail provided for higher-impact systems than for lower-impact systems. Organizations use discretion in applying the security controls to information systems, giving consideration to the scalability factors in particular environments. This approach facilitates a cost-effective, risk-based approach to security control implementation that expends no more resources than necessary, yet achieves sufficient risk mitigation and adequate security.

Document the Decisions in the Security Plan

The information system owner documents the decisions made during the security control selection process, providing a sound rationale for each decision. This documentation is essential when examining the overall security considerations for the information system with respect to potential mission or business impact.

When documenting the selected set of security controls in the security plan, the extent and rigor of the rationales provided in the plan are scaled to the system's impact level with significantly less explanation needed for a low-impact system than for a high-impact system.

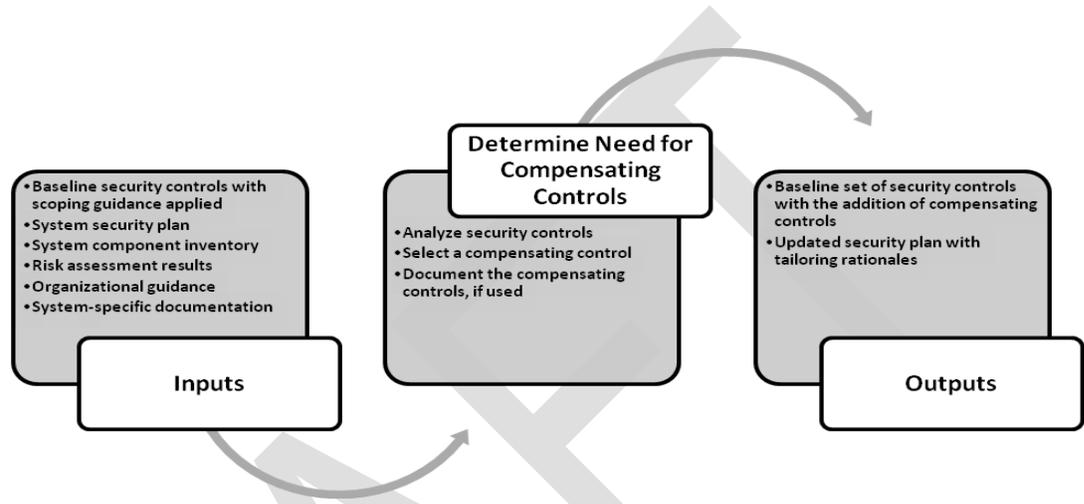
NO.	CONTROL NAME	TAILORING	RATIONALE
AC-1	Access Control Policy and Procedure	Common control	Common control-related consideration: The organization's security policies and procedures document implements this security control. See the information security program office for assessment results.
....			
AC-3	Account Enforcement	FIPS 140 does not apply	Policy/regulatory-related consideration: Encryption of stored information is not employed as an access enforcement mechanism; therefore, FIPS 140-2 (as amended) does not apply.
....			
AT-3	Security Training	Common control	Common control-related consideration: The information security program office provides role-based security training that is sufficient for the information system

			users. See the information security program office for assessment results.
AT-4	Security Training Records	Common control	Common control-related consideration: The information security program office provides a training record tool that manages organizational training records. See the information security program office for assessment results.
....			
CP-2	Contingency Plan	Hybrid control	Common control-related consideration: The information security program office provides training on how to develop an information system contingency plan and a standard template for all systems within the organization. The contingency plan template is completed by the information system owner as part of security documentation for the information system.
CP-2(1)	Contingency Plan	Downgraded to CP-2	Security objective-related consideration: While the information system's impact level is moderate, the security category for availability is low; therefore, CP-2(1) can be eliminated without impacting the security posture for the information system. CP-2, required in low-impact systems, is sufficient.
CP-3	Contingency Training	None	Security objective-related consideration: The information system's impact level is moderate and the security category for availability is low, but based on the risk assessment results, this security control is not downgraded and will be implemented within the information system. See security plan section XYZ for details.
....			
IA-3	Device Identification and Authentication		
IA-4	Identifier Management	Component	Public access-related consideration: The requirement for a security control identifier does not apply to those information system users that are accessing the public website to obtain publically-available information.
....			
PE-14	Temperature and Humidity Controls	Component	Physical infrastructure-related consideration: The temperature and humidity controls do not apply to the remote sensors implemented in the information system.
PE-15	Water Damage Protection	Hybrid control / Component	Physical infrastructure-related consideration: Water damage protection is provided to the portions of the information system that are housed within the data center. The remote sensors are designed to withstand water damage and do not need to implement PE-15.
....			
SC-12	Cryptographic Key Establishment and Management	Does not apply	Technology-related consideration: The information system does not employ cryptography.
SC-13	Use of Cryptography	Does not apply	Technology-related consideration: The information system does not employ cryptography.
....			
SI-11	Error Handling		

SI-12	Information Output Handling and Retention		
-------	---	--	--

DETERMINE NEED FOR COMPENSATING CONTROLS

Compensating controls are another method for tailoring the system’s security controls. A compensating security control is a management, operational, or technical control used by an organization instead of a recommended security control in the low, moderate, or high baseline that provides equivalent or comparable protection for an information system. The use of a compensating control is documented in the security plan.



Analyze Security Controls

Each security control is analyzed to determine if there is a control or part of a control that cannot be implemented in the information system due to technical infeasibility or cost associated with implementing the security control. If there is a security control that cannot be met, the information system owner identifies the effect failing to implement the control will have on the system’s security posture. The information system owner determines alternate methods or actions (i.e., a compensating control) that can be used to provide equivalent or comparable protection to the system. For example, additional operational procedures can be implemented or an alternate technical solution can be used.

Select a Compensating Control

When selecting an appropriate compensating control, the information system owner first determines if an alternate control (or group of controls) can be selected from the NIST SP 800-53, Appendix F security control catalog. Every attempt should be made to select the compensating control from the NIST security control catalog, but if an appropriate security control cannot be found in the catalog, a suitable control from another source may be selected. The organization formally accepts the risks associated with employing the compensating control in the information system.

Document the Compensating Controls

The spreadsheet/table is updated to note that the control is implemented as a compensating control. The rationale for the compensating control includes a complete and convincing rationale for how the compensating control provides an equivalent security capability or level of protection for the information system and why the original security control could not be employed. The compensating control numbers and names are included in the compensating control rationale.

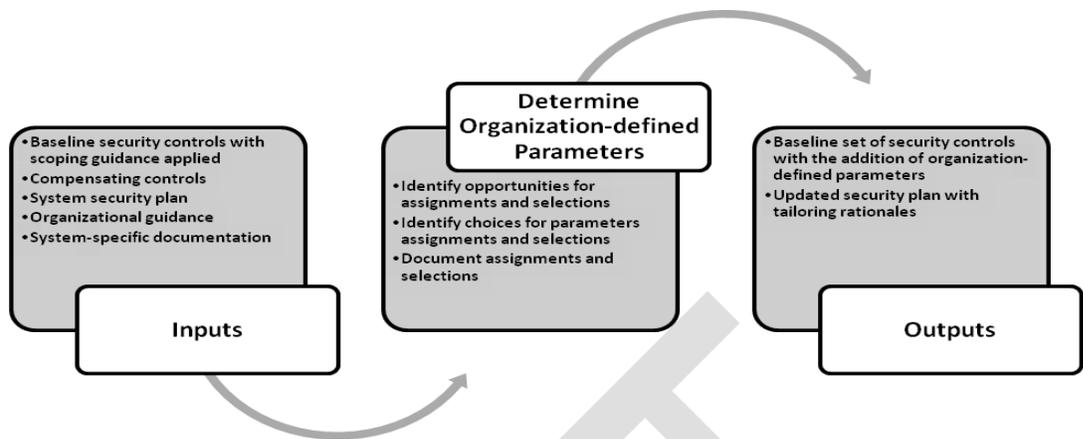
The sample spreadsheet/table has been updated with a compensating control, the source of the compensating control, and supporting rationale.

NO.	CONTROL NAME	TAILORING	RATIONALE
AC-1	Access Control Policy and Procedure	Common control	Common control-related consideration: The organization's security policies and procedures document implements this security control. See the information security program office for assessment results.
....			
AC-3	Account Enforcement	FIPS 140 does not apply	Policy/regulatory-related consideration: Encryption of stored information is not employed as an access enforcement mechanism; therefore, FIPS 140-2 (as amended) does not apply.
....			
AT-3	Security Training	Common control	Common control-related consideration: The information security program office provides role-based security training that is sufficient for the information system users. See the information security program office for assessment results.
AT-4	Security Training Records	Common control	Common control-related consideration: The information security program office provides a training record tool that manages organizational training records. See the information security program office for assessment results.
....			
CP-2	Contingency Plan	Hybrid control	Common control-related consideration: The information security program office provides training on how to develop an information system contingency plan and a standard template for all systems within the organization. The contingency plan template is completed by the information system owner as part of security documentation for the information system.
CP-2(1)	Contingency Plan	Downgraded to CP-2	Security objective-related consideration: While the information system's impact level is moderate, the security category for availability is low; therefore, CP-2(1) can be eliminated without impacting the security posture for the information system. CP-2, required in low-impact systems, is sufficient.
CP-3	Contingency Training	None	Security objective-related consideration: The information system's impact level is moderate and the security category for availability is low, but based on the risk assessment results, this security control is not downgraded and will be implemented within the information system. See security plan section XYZ for details.
....			
IA-3	Device Identification and Authentication		
IA-4	Identifier Management	Component	Public access-related consideration: The requirement for a security control identifier does not apply to those information system users that are accessing the public website to obtain publically-available information.
....			
PE-2(1)	Physical Access Control	Compensating Control	This control was added to compensate for SI-11, Error Handling.

....			
PE-14	Temperature and Humidity Controls	Component	Physical infrastructure-related consideration: The temperature and humidity controls do not apply to the remote sensors implemented in the information system.
PE-15	Water Damage Protection	Hybrid control / Component	Physical infrastructure-related consideration: Water damage protection is provided to the portions of the information system that are housed within the data center. The remote sensors are designed to withstand water damage and do not need to implement PE-15.
....			
SC-12	Cryptographic Key Establishment and Management	Does not apply	Technology-related consideration: The information system does not employ cryptography.
SC-13	Use of Cryptography	Does not apply	Technology-related consideration: The information system does not employ cryptography.
....			
SI-11	Error Handling	Compensating control	It is infeasible to implement the error handling capability in the information system due to the development cost to add this capability to the 17-year old information system. This capability is planned for the replacement system that is expected to be operational within the next two years. Equivalent security is provided by PE-2(1), Physical Access Control, where the physical access to the information system components are restricted in addition to the physical security restrictions to the facility.
SI-12	Information Output Handling and Retention		

DETERMINE ORGANIZATION-DEFINED PARAMETERS

Security controls containing organization-defined parameters (i.e., assignment or selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives. Where specified, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, Executive Orders, directives, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk. The organization-defined security control parameters are documented in the security plan.



Identify Opportunities for Assignments and Selections

Each security control is reviewed to determine if there is a need to make an assignment or selection within the security control. If there is an opportunity for an assignment or selection, the information system owner determines what has to be assigned/selected (e.g., how the system reacts after an organization-assigned number of unsuccessful logon attempts, the frequency of security awareness training, the list of prohibited or restricted functions, ports, protocols, or services, what events should be audited) and the appropriate values to provide adequate protection for the information system.

Identify Choices for Parameter Assignments and Selections

The information security program office or component/department may have made the assignment and selection decisions for the organization’s information systems to ensure consistency throughout the organization. If the organization has already assigned a value to an assignment/selection parameter, the information system owner analyzes the choice to determine if it is suitable for the information system (i.e., does it meet the system’s requirements for the selection or assignment). If the organization has not made an assignment/selection for the parameter or the assignment is not suitable for the system, the information system owner determines the appropriate choice for the assignment/selection by reviewing best security practices, other applicable NIST guidance or configuration checklists, OMB directives, and organizational guidance on determining the parameter values.

Document Assignments and Selections

If an assignment/selection was made for any of the security controls, the spreadsheet/table is updated to note that an assignment/selection has been made and the assignment/selection choice.

The sample spreadsheet/table has been updated with the assignments and selections.

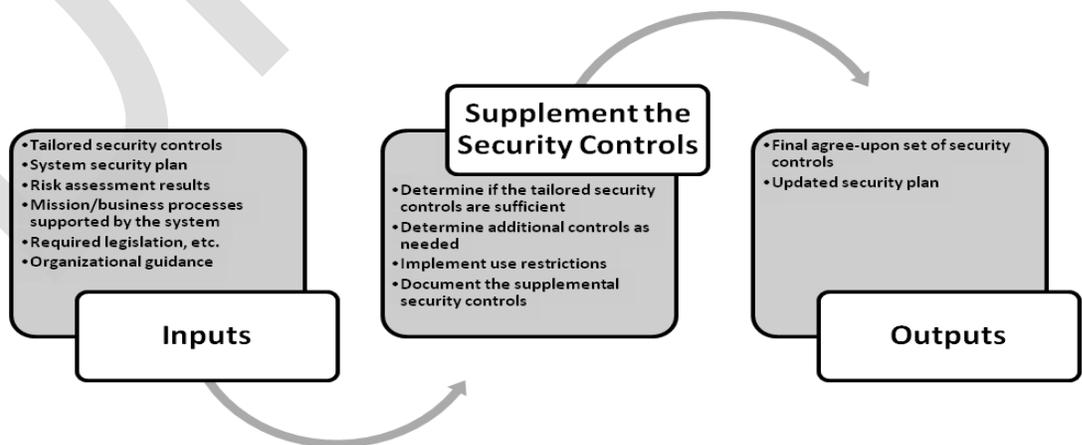
NO.	CONTROL NAME	TAILORING	RATIONALE
AC-1	Access Control Policy and Procedure	Common control	Common control-related consideration: The organization’s security policies and procedures document implements this security control. See the information security program office for assessment results.
....			
AC-3	Account Enforcement	FIPS 140 does not apply	Policy/regulatory-related consideration: Encryption of stored information is not employed as an access enforcement mechanism; therefore, FIPS 140-2 (as amended) does not apply.
....			

AT-3	Security Training	Common control Organization-defined Parameter	Common control-related consideration: The information security program office provides role-based security training that is sufficient for the information system users. See the information security program office for assessment results. Assignment: Annual
AT-4	Security Training Records	Common control Organization-defined Parameter	Common control-related consideration: The information security program office provides a training record tool that manages organizational training records. See the information security program office for assessment results. Assignment: Five years
....			
CP-2	Contingency Plan	Hybrid control	Common control-related consideration: The information security program office provides training on how to develop an information system contingency plan and a standard template for all systems within the organization. The contingency plan template is completed by the information system owner as part of security documentation for the information system.
CP-2(1)	Contingency Plan	Downgraded to CP-2	Security objective-related consideration: While the information system's impact level is moderate, the security category for availability is low; therefore, CP-2(1) can be eliminated without impacting the security posture for the information system. CP-2, required in low-impact systems, is sufficient.
CP-3	Contingency Training	Organization-defined Parameter	Security objective-related consideration: The information system's impact level is moderate and the security category for availability is low, but based on the risk assessment results, this security control is not downgraded and will be implemented within the information system. See security plan section XYZ for details. Assignment: Every two years
....			
IA-3	Device Identification and Authentication	Organization-defined Parameter	Assignment: Web servers
IA-4	Identifier Management	Component Organization-defined Parameter	Public access-related consideration: The requirement for a security control identifier does not apply to those information system users that are accessing the public website to obtain publicly-available information. Assignment: d. Two years e. 30 minutes
....			
PE-2(1)	Physical Access Control	Compensating Control	This control was added to compensate for SI-11, Error Handling.
....			
PE-14	Temperature and Humidity Controls	Component Organization-defined Parameter	Physical infrastructure-related consideration: The temperature and humidity controls do not apply to the remote sensors implemented in the information system. Assignment: a. temperature range, 68 - 77 ° Fahrenheit; humidity range, 40-55%
PE-15	Water Damage Protection	Hybrid control /	Physical infrastructure-related consideration:

		Component	Water damage protection is provided to the portions of the information system that are housed within the data center. The remote sensors are designed to withstand water damage and do not need to implement PE-15.
....			
SC-12	Cryptographic Key Establishment and Management	Does not apply	Technology-related consideration: The information system does not employ cryptography.
SC-13	Use of Cryptography	Does not apply	Technology-related consideration: The information system does not employ cryptography.
....			
SI-11	Error Handling	Compensating control	It is infeasible to implement the error handling capability in the information system due to the development cost to add this capability to the 17-year old information system. This capability is planned for the replacement system that is expected to be operational within the next two years. Equivalent security is provided by PE-2(1), Physical Access Control, where the physical access to the information system components are restricted in addition to the physical security restrictions to the facility.
SI-12	Information Output Handling and Retention		

SUPPLEMENT THE SECURITY CONTROLS

The tailored security control baseline should be viewed as the foundation or starting point for determining the needed set of security controls for an information system. The risk assessment results provide important inputs to determine the sufficiency of the security controls in the tailored baseline—that is, determining whether or not the security controls adequately protect the organization’s operations and assets, individuals, other organizations, and the Nation. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations.



Determine if the Tailored Baseline is Sufficient

The information system owner evaluates the tailored baseline of security controls to determine if they are sufficient to meet the needs of the information system. Using the risk assessment results, mission/business requirements, and system description, the information system owner reviews potential threats, vulnerabilities, and resulting information system risks and applicable laws, Executive Orders, directives, policies, standards, or regulations, including organization-specific guidance to determine if additional security controls or control enhancements are necessary to adequately protect the information system.

Define Additional Controls as Needed

If the information system owner determines that additional security controls are needed, they should be selected from Appendix F in the NIST SP 800-53 security control catalog. The catalog contains numerous controls and control enhancements that are found only in higher impact baselines or are not included in any of the baselines. If additional security controls or compensating controls cannot be identified to effectively protect the information system, system use restrictions are considered.

In some cases instead of adding security controls, the implementation of the security control can be modified. Implementation modifications could include increasing the frequency that security activities are conducted, increasing the level of detail and scope in security documentation or operating procedures, or increasing the frequency of security reporting during continuous monitoring.

Implement Use Restrictions

If the organization cannot apply sufficient security controls within the information system to adequately reduce or mitigate risk, use restrictions are applied. Restrictions on the types of technologies used and how the information system is employed provide an alternative method to reduce or mitigate risk when security controls cannot be implemented within technology/resource constraints, or when controls lack reasonable expectation of effectiveness against identified threat sources. Restrictions on the use of information systems and specific information technologies are in many situations the only practical or reasonable course of action an organization can take in order to have the ability to carry out its assigned missions and business functions in the face of determined adversaries.

Document the Supplemental Security Controls

The supplemental security controls are added to the spreadsheet/table with the tailored security controls to represent the final, selected set of security controls. The rationale for supplementing a control includes the reasons for the supplementation, where the supplemental control came from (e.g., NIST SP 800-53, Appendix F, organization-specific policy guidance, OMB regulation), and how the supplemental control addresses the information system requirements.

The sample spreadsheet/table has been updated with supplemental controls along with the supporting rationale.

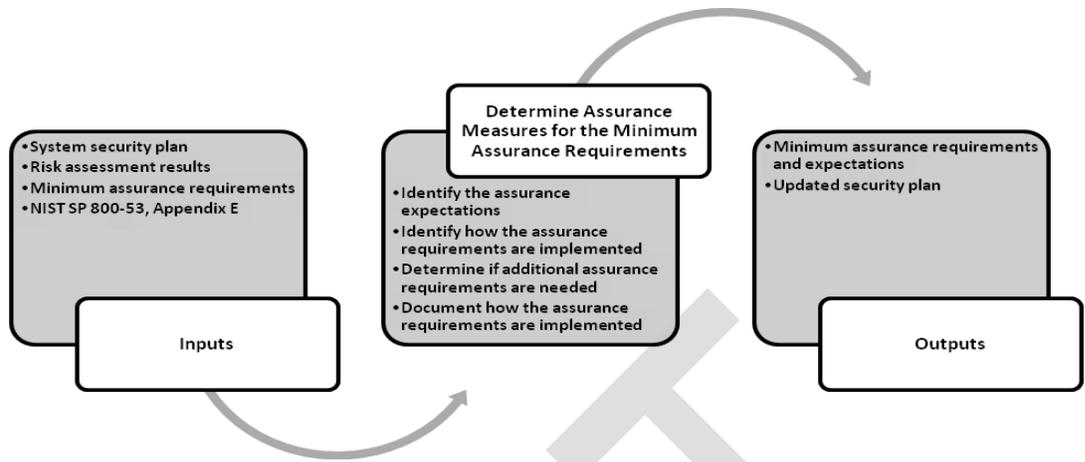
NO.	CONTROL NAME	TAILORING	RATIONALE
AC-1	Access Control Policy and Procedure	Common control	Common control-related consideration: The organization's security policies and procedures document implements this security control. See the information security program office for assessment results.
....			
AC-3	Account Enforcement	FIPS 140 does not apply	Policy/regulatory-related consideration: Encryption of stored information is not employed as an access enforcement mechanism; therefore, FIPS 140-2 (as amended) does not apply.

....			
AT-3	Security Training	Common control Organization-defined Parameter	Common control-related consideration: The information security program office provides role-based security training that is sufficient for the information system users. See the information security program office for assessment results. Assignment: Annual
AT-4	Security Training Records	Common control Organization-defined Parameter	Common control-related consideration: The information security program office provides a training record tool that manages organizational training records. See the information security program office for assessment results. Assignment: Five years
....			
AU-10(1)	Non-Repudiation	Supplemental control	Based on the risk assessment, this control is added to the baseline. This information system supports law enforcement activities and specific actions within the information system must be logged and reviewed.
....			
CP-2	Contingency Plan	Hybrid control	Common control-related consideration: The information security program office provides training on how to develop an information system contingency plan and a standard template for all systems within the organization. The contingency plan template is completed by the information system owner as part of security documentation for the information system.
CP-2(1)	Contingency Plan	Downgraded to CP-2	Security objective-related consideration: While the information system's impact level is moderate, the security category for availability is low; therefore, CP-2(1) can be eliminated without impacting the security posture for the information system. CP-2, required in low-impact systems, is sufficient.
CP-3	Contingency Training	Organization-defined Parameter	Security objective-related consideration: The information system's impact level is moderate and the security category for availability is low, but based on the risk assessment results, this security control is not downgraded and will be implemented within the information system. See security plan section XYZ for details. Assignment: Every two years
....			
IA-3	Device Identification and Authentication	Organization-defined Parameter	Assignment: Web servers
IA-4	Identifier Management	Component Organization-defined Parameter	Public access-related consideration: The requirement for a security control identifier does not apply to those information system users that are accessing the public website to obtain publically-available information. Assignment: d. Two years e. 30 minutes
....			
PE-2(1)	Physical Access Control	Compensating Control	This control was added to compensate for SI-11, Error Handling.
....			
PE-14	Temperature and Humidity Controls	Component	Physical infrastructure-related consideration:

		Organization-defined Parameter	The temperature and humidity controls do not apply to the remote sensors implemented in the information system. Assignment: a. temperature range, 68 - 77 ° Fahrenheit; humidity range, 40-55%
PE-15	Water Damage Protection	Hybrid control / Component	Physical infrastructure-related consideration: Water damage protection is provided to the portions of the information system that are housed within the data center. The remote sensors are designed to withstand water damage and do not need to implement PE-15.
....			
SA-12	Supply Chain Protection	Supplemental control	Based on the risk assessment, this control is added to the baseline. This information system supports law enforcement activities and requires that the information technology products within the system be from known/approved sources.
....			
SC-12	Cryptographic Key Establishment and Management	Does not apply	Technology-related consideration: The information system does not employ cryptography.
SC-13	Use of Cryptography	Does not apply	Technology-related consideration: The information system does not employ cryptography.
....			
SI-11	Error Handling	Compensating control	It is infeasible to implement the error handling capability in the information system due to the development cost to add this capability to the 17-year old information system. This capability is planned for the replacement system that is expected to be operational within the next two years. Equivalent security is provided by PE-2(1), Physical Access Control, where the physical access to the information system components are restricted in addition to the physical security restrictions to the facility.
SI-12	Information Output Handling and Retention		

DETERMINE ASSURANCE MEASURES FOR THE MINIMUM ASSURANCE REQUIREMENTS

Assurance is the grounds for confidence that the security controls implemented within an information system are effective in their application. Assurance can be obtained in a variety of ways, including actions taken by developers, implementers, and operators in the specification, design, development, implementation, operation, and maintenance of security controls. Assurance is also obtained by the actions taken by security control assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.



Identify the Assurance Expectations for Security Control Baselines

The minimum assurance expectations are defined in NIST SP 800-53, Appendix E. For security controls in low-impact information systems, the focus is on the controls being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

For security controls in moderate-impact information systems, the focus is on actions supporting increased confidence in the correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation supporting increased confidence that the control meets its required function or purpose. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

For security controls in high-impact information systems, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control’s effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. This documentation is also needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Identify How the Minimum Assurance Requirements are Implemented

Assurance requirements are directed at security control developers/implementers. Based on the assurance requirements, security control developers/implementers carry out required activities and, as an inherent part of developing or implementing the control, produce the necessary control documentation, conduct essential analyses, and define actions that are performed during control operation. The purpose of these activities is to provide increased grounds for confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Assessors subsequently use the information from these developer/implementer activities during the Assess Step to help build the assurance case that the security controls are effective in their application.

Developer/implementer actions to meet the assurance requirements can include:

- Identifying mechanisms/automated functions that will be implemented in the system’s hardware, software, or firmware (e.g., encryption, access control, information flow control);

- Defining specifications or document-base artifacts (e.g., contingency plan, incident handling policy and procedures) that need to be written; or
- Specifying activities or actions that will be conducted by people (e.g., update risk assessment, conduct contingency testing, conduct server maintenance, maintain training records) when the system is in operation.

Each security control is reviewed to determine the additional actions or documentation needed to address the assessment expectations. For example, all organizations are expected to implement CM-4, Security Impact Analysis. For a high-impact information system to demonstrate implementation of the assurance requirements, the organization is expected to prepare documentation that shows the security impact analysis procedures are sufficient to meet their function and purpose. In addition, there is a process in place within the organization to capture lessons learned as they relate to security impact analysis and update the related policies and procedures to ensure a more consistent implementation throughout the organization.

**Determine if
Additional
Assurance
Requirements are
Needed**

NIST SP 800-53, Appendix E, also contains additional assurance requirements available to developers/implementers of security controls that supplement the minimum assurance requirements for moderate- and high-impact information systems. These additional assurance requirements are needed in order to protect against threats from highly skilled, highly motivated, and well-resourced threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risk associated with the highly skilled, highly motivated, and well-resourced threat agents.

**Document How the
Minimum
Assurance
Requirements are
Implemented**

The information system owner also includes in each security control description any actions that are required to implement the assurance requirements. For example, all organizations are required to implement IR-6, Incident Reporting. For a low-impact system it may be sufficient to issue procedures for personnel to use to report security incidents to designated authorities. For a moderate-impact system, it may be necessary to document additional incident response policies and procedures that assign specific roles and responsibilities for individuals within the organization and to require those implementing the procedures to maintain records to demonstrate that the incidents have been properly reported and handled. For a high-impact system, the organization is also expected to implement a mechanism to capture lessons learned during the reporting process and continuously improve the incident reporting process.

When documenting in the security plan how the assurance requirements are implemented in the information system, the extent of the description should be scaled to the system's impact level with significantly less explanation needed for a low-impact system than for a high-impact system. There should be sufficient detail to enable a compliant implementation of the minimum assurance requirements. For example, the assurance requirements' implementation description (for the sample moderate-impact information system) is documented in the security plan along with the information on the control implementation.⁴

Section XYZ

CP-3, Contingency Training

Control Implementation: Contingency training is planned for every 18 months to 2 years for System ABC. The System ABC Program Office prepares a System ABC Contingency Training plan that includes the information recommended in NIST SP 800-34, *Contingency Planning Guide for Information*

⁴ This sample shows one way that the planned implementation of the security control and minimum assurance requirements can be documented in the system security plan. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-37.

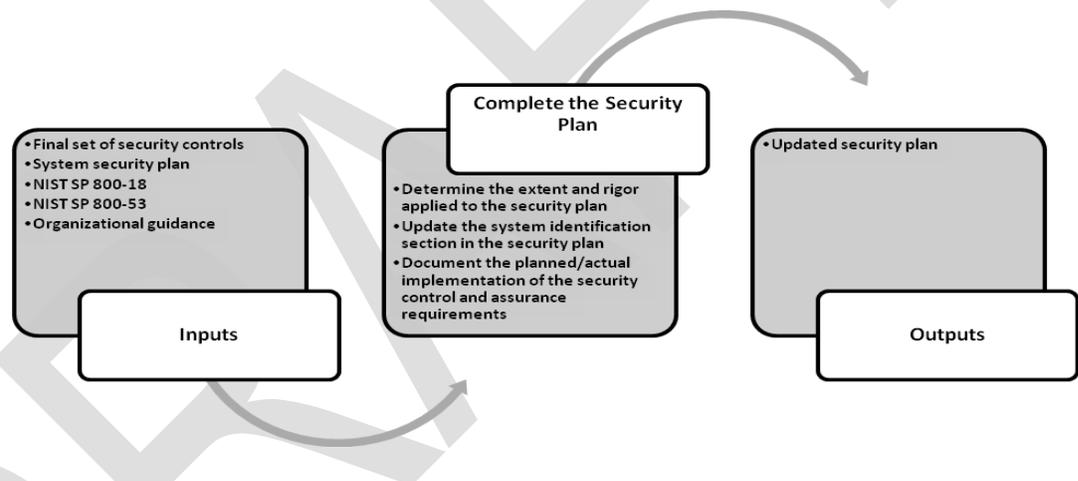
Technology Systems. The actions necessary to plan for and conduct the contingency training, including the coordination with the information technology provider, are documented in the training plan.

Minimum Assurance Requirement Implementation: To meet the minimum assurance requirements, the following are defined prior to implementation and included in contract specifications, if the contingency training services are supplied by an external source:

- Level of detail required within the ABC System Contingency Training Plan;
- Documentation history recorded within the ABC System Contingency Training Plan;
- Records required to document training activities;
- Information that should be included in the training records; and
- Length of time the training records must be maintained.

COMPLETE THE SECURITY PLAN

The information system owner documents the decisions made during the initial security control selection, tailoring, and supplementation processes in the security plan, providing a sound rationale for those decisions. This documentation is essential when examining the overall security considerations for information systems with respect to potential mission or business case impact. The resulting set of selected security controls along with the supporting rationale for control selection decisions and any information system use restrictions are documented in the system security plan.



Determine the Extent and Rigor Applied to the Security Plan

The security plan is scalable with regard to the extent and rigor of the implementation. The scalability is guided by the security categorization decisions, where the security plan for a high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, the security plan for a low-impact information system may be considerably shorter and contain much less implementation detail.

Update the System Identification Section in the Security Plan

The system identification section of the security plan includes the descriptive information about the information system as defined in NIST SP 800-37. Alternatively, the system description information can be included in an attachment to the security plan or referenced in other standard sources for information generated as part of the system development life cycle. Information should be added to this section as it becomes available during the system development life cycle and the execution of the Risk Management Framework tasks.

It is imperative to document any significant risk management decisions made during the security control selection process in order for authorizing officials to have the necessary information to make credible, risk-based decisions regarding the authorization of organizational information systems. In addition, without such information, the

understanding, assumptions, and rationale supporting those important risk decisions will, in all likelihood, not be available when the state of the information systems or environment of operation changes, and the original risk decisions are revisited.

Document the Planned or Actual Implementation of the Security Controls and Minimum Assurance Requirements

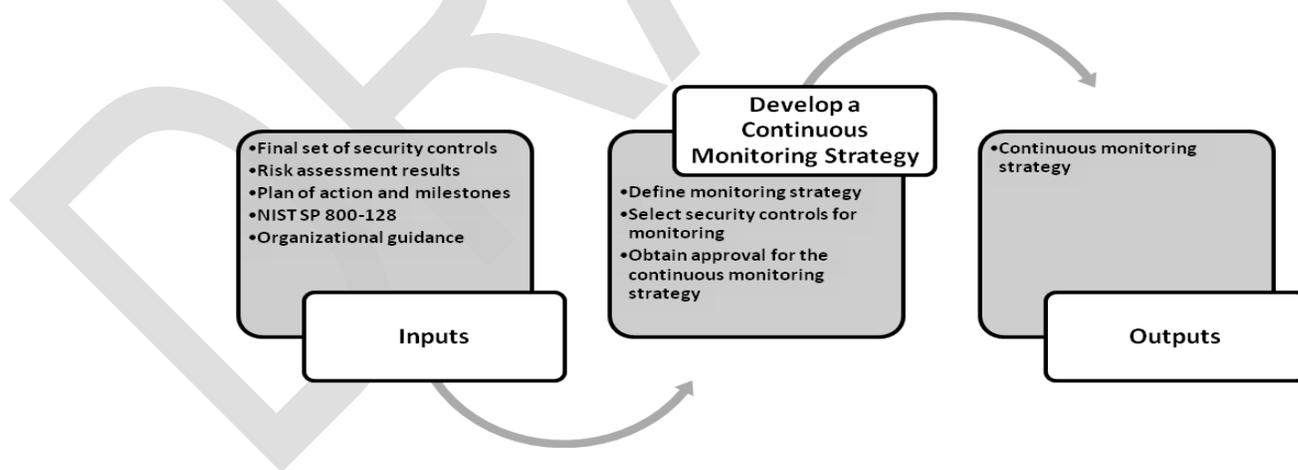
In addition to the list of security controls to be implemented, the security plan describes the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the control. This section identifies each selected security control by number and title with the planned or actual implementation. As the information system progresses through the system development life cycle, the security plan is updated to reflect any modifications to the security controls based on the risk mitigation activities carried out by the information system owner.

The minimum assurance requirements are applied on a control-by-control basis; therefore, the information system owner also includes in each security control description any actions that are required to implement the minimum assurance requirements. The implementation of the minimum assurance requirements is also updated during the system development life cycle to reflect any changes within the information system.

DEVELOP A CONTINUOUS MONITORING STRATEGY

During the Select Step, the information system owner or common control provider initiates development of the continuous monitoring strategy to manage the ongoing monitoring of security controls employed within or inherited by an information system. The ongoing monitoring program allows an organization to track the security state of an information system on a continuous basis and maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and mission/business processes.

An effective monitoring program includes: (i) configuration management and control processes; (ii) security impact analyses on proposed or actual changes to the information system and its environment of operation; (iii) assessment of selected security controls employed within and inherited by the information system (including controls in dynamic subsystems); and (iv) security status reporting to appropriate organizational officials.



Define Monitoring Strategy

Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment. The monitoring strategy defines how changes to the information system will be monitored and how the security impact analyses will be conducted. The information system owner or common control provider determines their approach to managing proposed changes to their information systems or supporting operating environment that is consistent with the organization’s configuration management process.

The continuous monitoring strategy also addresses the need to determine the extent to which a proposed change to the system or its operating environment will affect the security state of the system. The information system owner establishes when security impact analyses are conducted, what type of proposed changes or configuration settings should be analyzed, how the proposed changes will be analyzed, what information about the analysis should be recorded, and how it will be recorded.

Information systems are also expected to conform to organizationally approved configurations that are maintained throughout the system's life cycle. Tools, such as Security Content Automation Protocol (SCAP)-validated products, help to manage system configurations. These tools, when available, are used to determine whether the configuration settings applied to system components comply with government standards and policies.

Select Security Controls for Monitoring

A critical aspect of the continuous monitoring strategy is the ongoing monitoring of the security controls employed within or inherited by the information system. The strategy identifies the security controls to be monitored, the frequency of monitoring, and the control assessment approach.

The information system owner and common control provider, in collaboration with organizational officials include the authorizing official, chief information officer, senior information security officer, and risk executive (function), identify the criteria for selecting security control to be monitored post deployment and determine the frequency of the monitoring.

The selection criteria reflect the priorities and importance of the information system to organizational operations and assets, individuals, other organizations, and the Nation. Security control that are volatile (i.e., most likely to change over time), critical to certain aspects of the organization's protection strategy, or identified in current plans of action and milestones are assessed as frequently as necessary consistent with the criticality of the function and capability of the monitoring tools.

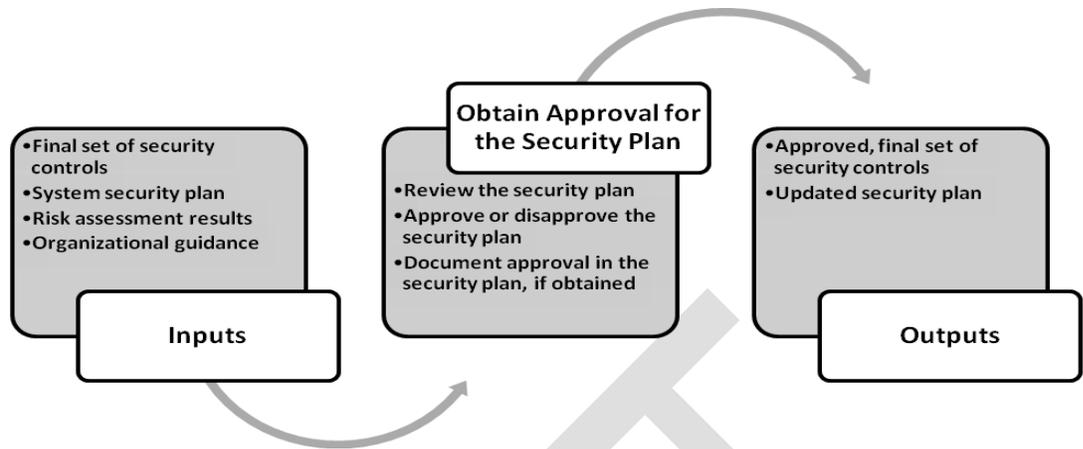
The continuous monitoring strategy can be documented in the system security plan or other appropriate document.

Obtain Approval for the Continuous Monitoring Strategy

Approval for the continuous monitoring strategy can be obtained in conjunction with the approval of the security plan. When available, using automated tools and supporting databases to conduct the continuous monitoring activities facilitates near real-time risk management for the information system and represents a significant change in the way security authorization activities have been employed in the past.

OBTAIN APPROVAL FOR THE SECURITY PLAN

The authorizing official determines if the security plan is complete, consistent, and satisfies the stated security requirements for the information system. Complete coverage of security controls in appropriate security plans facilitates more comprehensive information security, promotes increased accountability, provides an effective vehicle to better manage the risks resulting from the operation and use of information systems, and is required to adequately support the security assessment of systems as part of the security authorization process.



Review the Security Plan

The authorizing official determines, to the greatest extent possible with available planning or operational documents, if the security plan correctly and effectively documents the potential risk to organizational operations and assets, individuals, other organizations, and the Nation, that would be incurred if the controls identified in the plan were implemented as intended. Based on the results of this independent review and analysis, the authorizing official may recommend changes to the security plan.

Approve or Disapprove the Security Plan

If the security plan is deemed unacceptable, the authorizing official sends the plan back to the information system owner or common control provider for appropriate action. If the security plan is deemed acceptable, the authorizing official accepts the security plan. The acceptance of the security plan represents an important milestone in the risk management process. The authorizing official, by accepting the security plan, agrees to the set of security controls (system-specific, hybrid, or common controls) proposed to meet the security requirements for the information system. The agreement allows the risk management process to advance to the Implementation Step. The acceptance of the security plan also approves the level of effort required to successfully complete the remainder of the steps in the Risk Management Framework and provides the basis of the security specification for the acquisition of the information system, subsystems, or components.

Document Approval in the Security Plan

The approval of the security plan is documented within the plan and includes the names of reviewers and approvers of the document, the dates when the reviews/approvals took place, along with the type of approval (e.g., approval of supplemented baseline, authorization decision). Any comments or conditions for the approval are also documented in the security plan. The information system owner may provide a response to the review and approval results.

SELECTION SUMMARY

Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability requirements of the system and its information. The selection and implementation of appropriate security controls for an information system or a system-of-systems are important tasks that can have major implications on the operations and assets of an organization, as well as the welfare of individuals and the Nation.

Baseline controls are the starting point for the security control selection process and are chosen based on the security category and impact level of the information system. The tailored security control baseline (i.e., the appropriate control baseline from NIST SP 800-53, Appendix D adjusted in accordance with the tailoring guidance) is the minimum set of

security controls for the information system. Supplements to the tailored baseline will likely be necessary in order to achieve adequate risk mitigation. The tailored security control baseline is supplemented based on an organizational assessment of risk and the resulting controls documented in the security plan for the information system.

The minimum assurance requirements also levy additional expectations on security controls and are directed at the activities and actions that security control developers/implementers define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

The results of the security control selection process are documented in the system security plan and includes the following:

- Initial baseline of security controls
- Tailoring decisions with a supporting rationale (i.e., application of scoping guidance, selection of compensating controls, and identification of organization-defined parameters)
- Supplementation of security controls with supporting rationale
- Minimum assurance requirements and their impact on security control implementation
- Approval of the system security plan

REFERENCES

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Final Public Draft, December 2010
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, August 2009
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- Select FAQ, www.csrc.nist.gov/groups/SMA/fisma/Risk-Management--Framework/select/index.html