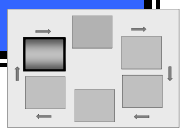
MONITOR STEP – TIPS AND TECHNIQUES FOR SYSTEMS



NIST RISK MANAGEMENT FRAMEWORK

Conducting a thorough point-in-time assessment of the security controls in an organizational information system is a necessary but not sufficient condition to demonstrate security due diligence. An effective continuous monitoring process integrated with the system development life cycle is needed to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as in the environment in which it operates. NIST SP 800-37, Revision 1, *Guide for the Authorization of Federal Information Systems: A Security Life Cycle*, Initial Public Draft, defines the requirements for the continuous monitoring process. A continuous monitoring program allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system. The information owner/information system owner[1] is responsible for monitoring their information systems, ensuring that the system authorization remains current, and updating critical security documents as changes to the system or operating environment occur.[2]

NOTE: These *Tips and Techniques for Systems* are provided as one example of how to implement continuous monitoring for information systems in accordance with NIST SP 800-37. Readers should understand that other implementations may be used to support their particular circumstances.

NIST SP 800-37 defines a security authorization process for information systems that consists of three phases: (i) the preparation phase; (ii) the execution phase; and (iii) the maintenance phase. The authorization maintenance phase defines the continuous monitoring process for the organization's information systems. The maintenance phase consists of nine tasks.

The tasks are: (i) develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes in the information system or its environment of operation; (ii) document the proposed or actual changes to the information system or the environment of operation; (iii) determine the security impact of the proposed of actual changes to the information system or the environment of operation in accordance with the security control monitoring strategy; (iv) assess a selected subset of the security controls in the information system or the environment of operation (including those controls affected by changes to the system/environment) in accordance with the continuous monitoring strategy; (v) conduct remediation actions based on the results of the selected security control assessments and outstanding items in the plan of action and milestones; (vi) update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process; (vii) report the security status of the information system to the authorizing official and other appropriate organizational officials on a periodic basis; (viii) periodically review the reported security status of the information system and determine whether the risk to organizational operations and assets, individuals, other organizations, or the nation remains acceptable; (ix) implement an organizationally approved information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

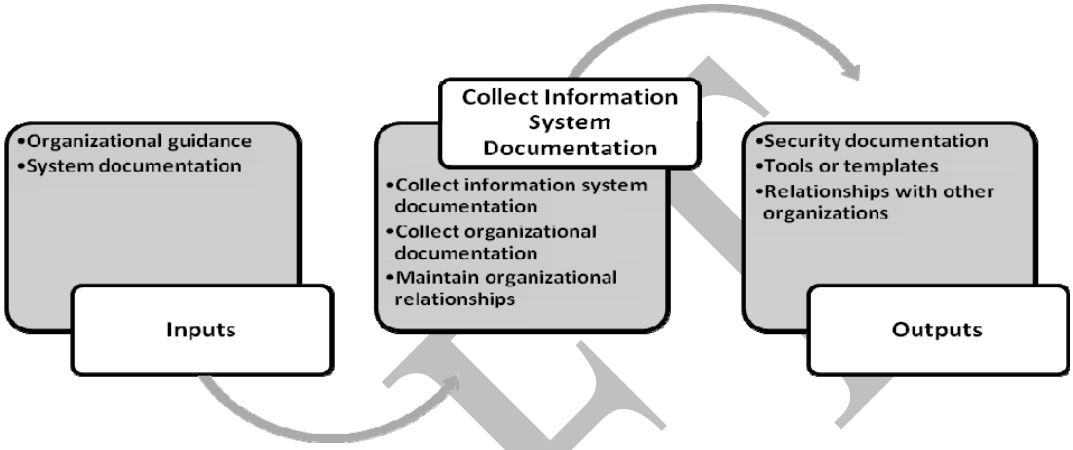
The tips and techniques in this document elaborate on the basic tasks and guidance in NIST SP 800-37 as examples for stimulating ideas in implementing continuous monitoring guidance in organization-specific and information system-specific environments.

[1] The common control provider conducts the same role as the information owner/information system owner to provide continuous monitoring for the common controls for which they are responsible.

[2] The information in the *Tips and Techniques* should be interpreted as one approach on how to implement the continuous monitoring process. Organizations may develop other methods to implement the NIST standards and guidance.

GATHER INFORMATION SYSTEM DOCUMENTATION

Continuous monitoring begins after an information system has been authorized to operate when security documentation such as the system security plan, plan of action and milestones, and other security related documentation (e.g., vulnerability scanning results, results of last contingency plan test) already exists. The information owner/information system owner should have or be able to obtain this information for the individuals responsible for the continuous monitoring of the information system.



Gather Information System Documentation

The information owner/information system owner should collect the security-related documents that were developed and updated throughout the system development life cycle. These documents include the system security plan, risk assessment, security assessment plan, security assessment report, plans of action and milestones, contingency plan, vulnerability scanning results, and any other available documents (e.g., system changes and their security impact analysis results).

Collect Organizational Documentation

Information owners/information system owners also need to obtain organization-wide guidance on how to conduct continuous monitoring for their information systems. Each organization may provide guidance that elaborates on the NIST standards and guidance and that includes details on how to conduct security impact analyses, configure their information systems, or select subsets of security controls for ongoing monitoring. The guidance may also provide organization-specific tools, templates, or checklists to support the continuous monitoring process as well as internal reporting and approval requirements.

Continue Organizational Relationships

In addition to gathering documentation, information owners/information system owners should continue their relationships with others within the organization. The information security program office serves as the primary contact for advice and support while monitoring individual information systems. They establish the organization-specific policies on continuous monitoring and provide any available tools, templates, or checklists to assist with the monitoring process.

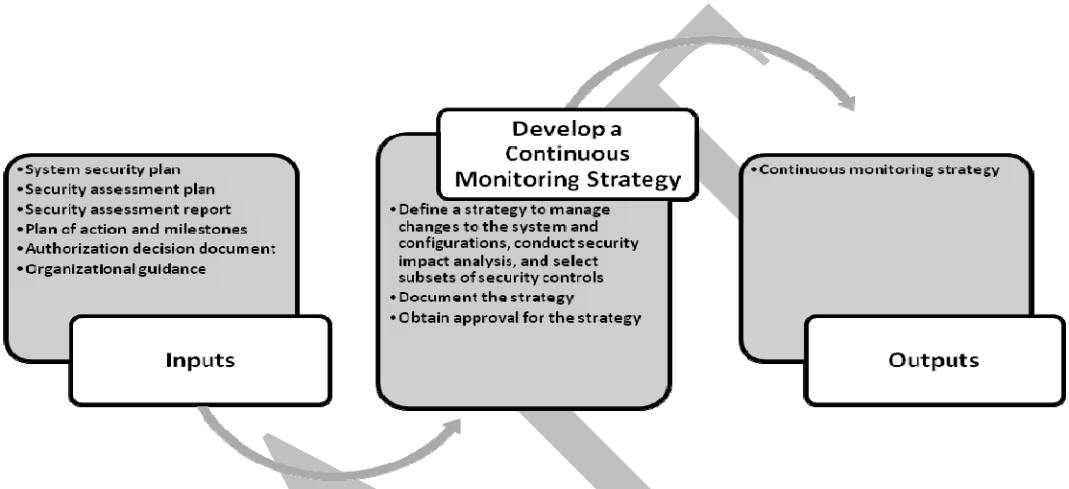
The information owner/information system owner also works with others within the organization including their information sharing partners and technical operations personnel. Each of these groups can help provide the information needed to effectively monitor an information system.

DRAFT

DEVELOP A CONTINUOUS MONITORING STRATEGY

The information owner/information system owner develops and documents a continuous monitoring strategy for their information systems. The continuous monitoring strategy can apply to an individual information system or for a group of related information systems.

Some organizations implement continuous monitoring as a common or hybrid security control. In those situations, the information owner/information system owner is expected to implement the organization-wide continuous monitoring strategy that may include the organizationally-defined security controls for ongoing monitoring.



Define Strategy to Manage Changes to the Information System

Information owners/information system owners determine their approach to managing proposed changes to their information systems or supporting operating environment that is consistent with the organization's configuration management process. If the organization implements configuration management as a common security control, the information owner/information system owner responsibilities are reduced.

If an organization-wide configuration management process is not available, information owners/information system owners will need to establish their own configuration management process or follow a configuration management process that is available for a group of information systems (e.g., all applications running on a mainframe, all information systems supporting the organization's financial operations). In addition, the information owner/information system owner will need to identify the types of changes that will be monitored. The information owner/information system owner should provide system users (e.g., mission/business representatives, system developers, system administrators, ISSOs) a standard template to request changes and capture the information needed to evaluate the proposed changes and the impacts of the proposed change on the system's performance and security posture.

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, should be used to determine whether the configuration settings applied to system components comply with government standards and policies.

DRAFT

Define Strategy for Conducting Security Impact Analysis

The continuous monitoring strategy should also address the requirement 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 owner/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.

Select Subsets of Security Controls for Monitoring

The information owner/information system owner also needs to select the subsets of security controls to be assessed and the number of subsets to be assessed during the authorization period that is based on the results of the last risk assessment, results of previous security assessments (including plans of action and milestones), and operational requirements unless the selection of controls for ongoing monitoring has been implemented as a common security control for the organization.

Priority should be given to security controls that are volatile, that have been identified in the system's plan of action and milestones, or that have been identified by senior leaders as having a significant impact on the organization. These controls should be assessed at least annually while other security controls should be assessed at least once during the authorization period. In addition, the level of assurance (or grounds for confidence) that the organization should have in determining the effectiveness of the security controls of the information system should also be considered when selecting which security controls to monitor and when in the authorization cycle the security controls should be monitored.

A table like the one below provides a convenient way to record the subset of security controls selected, the frequency of the control monitoring, and the schedule of the monitoring activities.[3] The table below is an extension of the sample table suggested in the Select Step – Tips and Techniques for Systems. During the Select Step of the Risk Management Framework, the security controls are selected and tailored to meet the needs of the information system and supporting operating environment. Using the table developed to record the security control selection and tailoring activities, additional information is added during the Monitor Step to document the selected subsets of controls for ongoing monitoring and the frequency of the monitoring activities.

In this example, AC-2 and IR-3 were deemed to be volatile or were identified in the plan of action and milestones as a weakness/deficiency in the information system and are monitored annually. Based on organizational guidance, IA-2 is monitored twice a year because of potential risk identified at the organizational level. The remaining controls are monitored at least once during the authorization cycle, following a schedule that fits the organization's needs and is consistent with the authorizing official's tolerance for risk.

In this example, the information system is originally authorized for operation in December of 2007. At the time of this chart, October 2008, the next review date is identified and planning should be in progress for reviews scheduled in December 2008. In addition to defining the frequency of security control monitoring, the events that could alter the security control selection and assessment schedule are identified and documented in the comments column.

Security Control No.	Control Name	Frequency	Review Dates	Comments
AC-1	Access Control Policy and Procedures	Once per authorization cycle	December 2010	
AC-2 (1)(2)(3)(4)	Account	Annually	December 2008	

DRAFT

	Management		December 2009 December 2010	
AT-3	Security Training	Once per authorization cycle	December 2009	
AT-4	Security Training Records	Once per authorization cycle	December 2009	
CP-2	Contingency Plan	Twice per authorization cycle	May 2009 December 2010	If an incident occurs that triggers use of the contingency plan, reassess this security control within two months of the incident
CP-3	Contingency Training	Once per authorization cycle	December 2010	
IA-2	User ID and Authentication	Semi-annually	May 2008 December 2008 May 2009 December 2009 May 2010 December 2010	Per organizational guidance
IR-3	Incident Response Testing and Exercises	Annually	December 2008 December 2009 December 2010	

Document the Continuous Monitoring Strategy

After the information owner/information system owner and authorizing official agree on the strategic decisions for continuous monitoring, the strategy is documented in a continuous monitoring plan, organizational policies and procedures, or another organizationally defined document. The documentation should identify the roles and responsibilities of those involved in the continuous monitoring process and the procedures that should be followed to effectively manage changes to the system. The documentation should also identify the subsets of security control that need to be assessed as well as the schedule by which the security control subsets should be assessed, The conditions that could alter the security controls included in a subset and the assessment schedule should also be defined.

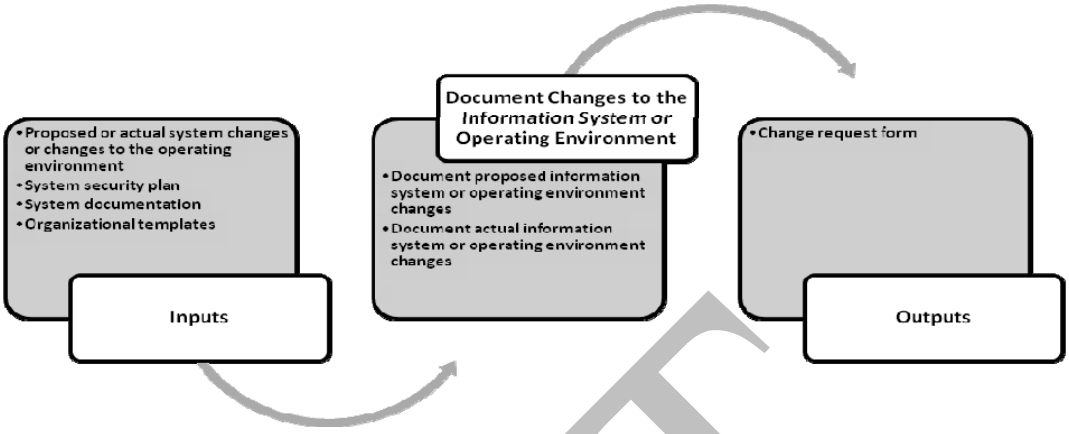
Obtain Approval for the Continuous Monitoring Strategy

The continuous monitoring strategy needs to be approved by the authorizing official and the senior agency information security officer. If the authorizing official or the senior agency information security officer has concerns about the continuous monitoring strategy, the information owner/information system owner works with them to establish an acceptable plan.

DOCUMENT CHANGES TO THE INFORMATION SYSTEM OR OPERATING ENVIRONMENT

Documenting proposed/actual changes to the information system or its operating environment and subsequently assessing the potential impact those changes may have on the overall security state of the system or the organization is an important aspect of security control monitoring, achieving situational awareness, and maintaining the security authorization. Information system changes should not be made prior to assessing the security impact of those changes.

DRAFT



Document Proposed Information System or Operating Environment Changes

The information owner/information system owner should document any relevant information about specific changes to the hardware, software, or firmware such as descriptions of planned new or modified features/capabilities or security implementation guidance. It is also important to document any proposed changes to the information system's operating environment such as modifications to hosting facilities or the organization's policies, processes, or procedures. The information owner/information system owner should use this information when assessing the potential security impact of the changes on the information system.

Proposed changes are typically documented in a change request form and include the following types of information:

- Change requestor's name and contact information;
- Description of the proposed change;
- Description of the problem that relates to the proposed change;
- Identification and description of any components affected by the change;
- Reason for the proposed change;
- Implications of not making the proposed change;
- Security controls impacted by the proposed change;
- Scope and impact of the proposed change on system or component operations;
- Types (e.g., local, remote) and number of users affected by the proposed change;
- Resource assessment of the proposed change (e.g., time and expertise required to implement the proposed change);
- Suggested implementation plan for the proposed change including proposed milestones;
- Back-out plan, including triggers for decision makers, if appropriate;
- Impacts on business continuity and contingency plans; and
- Risks involved in making the proposed change.

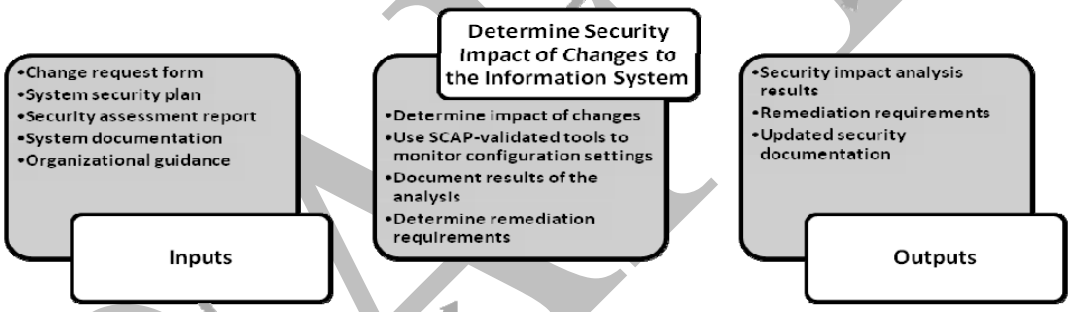
DRAFT

Document Actual Information System or Operating Environment Changes

Occasionally, a change that has not been included in a system change request or analyzed for its full impact on security will occur. It is still important to document the actual change (using the same change request form for proposed changes) to the information system or operating environment so that the security controls impacted by the change can be assessed. The information owner/information system owner should determine if the change can remain in the system, needs to be modified to maintain the system's security status, or should be removed from the system because it introduces an unacceptable level of risk to the information system or organization.

DETERMINE SECURITY IMPACT OF CHANGES TO THE INFORMATION SYSTEM

The information owner/information system owner needs to conduct security impact analyses to determine the extent to which changes to the information system or its operating environment will affect the security state of the system. Conducting security impact analyses is part of an ongoing assessment of risk. The effort applied to the security impact analysis should be commensurate with the information system's impact level and security category.



Determine Impact of Information System Changes

The information owner/information system owner, or a designated analysis team (consisting of members with a variety of expertise and system knowledge), should analyze each proposed change to the information system to determine what impact, if any, the proposed change has on the security posture of the information system. Changes to the information system or its operating environment may affect the security controls currently in place, produce new vulnerabilities in the system, or generate requirements for new security controls that were not previously needed. In assessing a change, the information owner/information system owner should consider the new or modified features/capabilities that the change will provide, any changes that should be made to the operating environment (e.g., updates to the rules of behavior, providing physical security of a new component), and the criticality of the change regarding system operation. Using the information gained during the analysis, the information owner/information system owner determines the security impact of the change on the information system.

Use SCAP-validated Tools to Monitor Configuration Settings

If the information system contains information technology components for which there exist SCAP-validated tools, the information owner/information system owner should use those tools to determine the compliance of each component's configuration with required standards such as the Federal Desktop Core Configuration (FDCC).[4] SCAP checklists (i.e., configuration checklists written in a checklist specification language (eXtensible Configuration Checklist Description Format, XCCDF) that have been accepted by the National Checklist Program) have compliance mappings embedded within the checklist so that SCAP-validated tools can automatically generate assessment and compliance

DRAFT

evidence linked to the NIST SP 800-53 security controls.

Document Results of the Security Impact Analysis

The information owners/information system owners document and share the results of the security impact analysis with the management and operations personnel, senior agency information security officer, and the risk executive (function) following an organizationally defined reporting format. The information owner/information system owner will use the information to decide whether to implement the proposed change to the information system. The senior agency information security officer and the risk executive (function) will use the information to determine the need for reauthorization of the information system and to identify organizational trends or patterns that impact the security of the organization.

Determine Remediation Actions Necessary Based on Security Impact Analysis

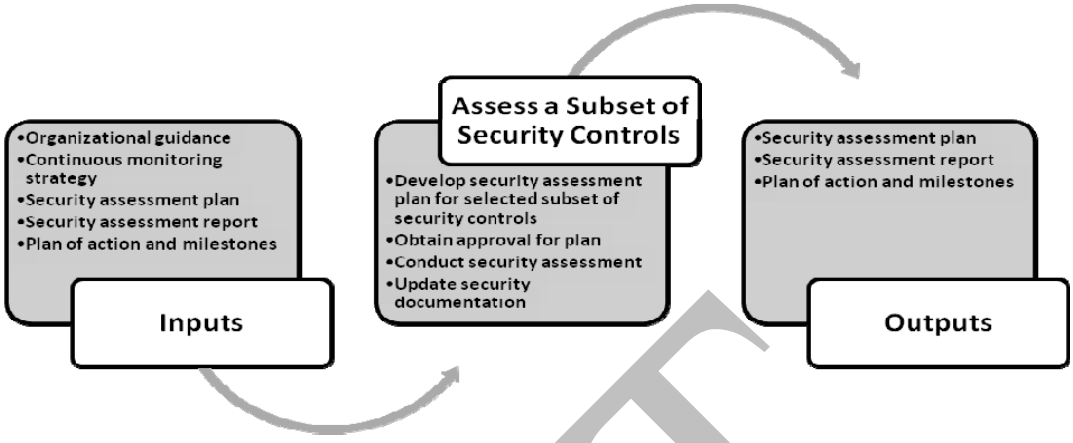
If the results of the security impact analysis indicate that the proposed change to the information system will affect the security state of the system, remediation actions or other changes should be initiated. For example, a change request proposes that a more recent version of a system component replace the current version of the component. The security impact analysis determined that the new component will not be configured to organizational standards. The resulting remediation actions require that the new component be properly configured prior to installing it in the operational system. The information owner/information system owner updates the plan of action and milestones to identify and track the remediation actions.

In another example, a common control provider reviews a new memorandum from OMB that specifies actions that each federal agency should implement. Based on the analysis, the common control provider determines that specific types of organizational servers should be reconfigured and that the organization's security awareness training should be revised to meet the new OMB requirements. The common control provider works with their technical operations personnel and the information security program office to implement the changes. After the changes are implemented, the common control provider updates the relevant security documentation and shares the results with the information owners/information system owners.

ASSESS A SUBSET OF SECURITY CONTROLS

During the continuous monitoring process, the information owner/information system owner assesses a subset of the system's security controls. The subsets of security controls and the schedule of security control assessments are defined in the continuous monitoring strategy. Security controls are assessed following previously developed security control assessment plans and procedures based on guidance identified in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*.

DRAFT



Develop Security Assessment Plan for Selected Subset of Security Controls

The continuous monitoring strategy defines the subsets of security controls and the assessment schedule for each control throughout the authorization period. The information owner/information system owner ensures a security control assessor with the appropriate knowledge, skills, and abilities evaluates the selected subset of security controls based on the defined assessment schedule. The degree of security control assessor independence required for the assessment during continuous monitoring should be determined by the authorizing official.

The security control assessor prepares the security assessment plan or revises an existing security assessment plan, selects the appropriate procedures from NIST SP 800-53A to assess the security controls, tailors the security assessment procedures to meet the organization's needs, develops additional procedures for organization-specific security controls or for additional assurance requirements, and optimizes the assessment procedures to conduct the assessment process efficiently.

Obtain Approval for Security Assessment Plan

After the security control assessor has completed the assessment plan, the plan is reviewed and approved by appropriate organizational officials (e.g., information owner/ information system owner, authorizing official, senior agency information security officer) to ensure that the plan is complete, is consistent with the security objectives of the organization, the organization's assessment of risk, and the system's continuous monitoring strategy, and is cost-effective with regard to the resources allocated for the assessment.

Conduct Security Assessment

The security control assessor executes the security assessment plan in accordance with the agreed-upon procedures, personnel, milestones, and schedule. The assessor provides unbiased, factual reporting of what was found for each security control assessed. For each finding of *other than satisfied*, the assessor identifies which requirements of the security control are affected by the finding and describes how the implementation or operation of the security control differs from the planned or expected security state.

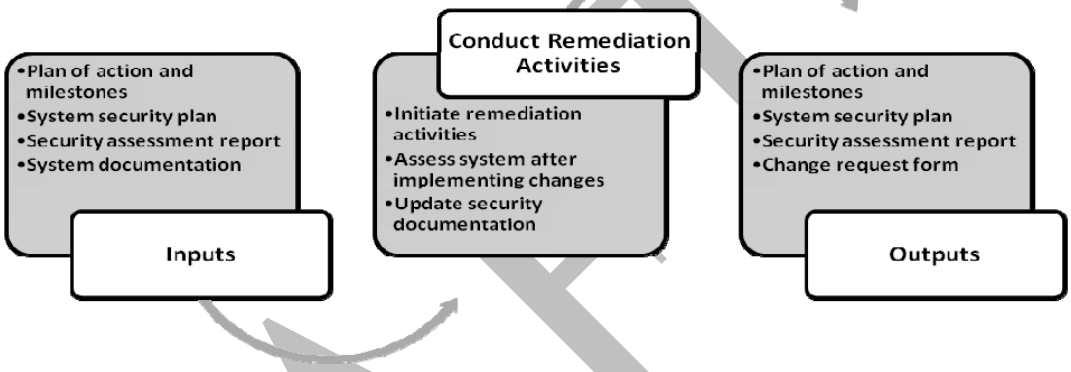
Update the Security Documentation

The security control assessor updates the security assessment report with the results of the latest assessment. The updated security assessment report should reflect the additional assessment activities carried out to determine security control effectiveness based on modifications to the security plan. The information owner/information system owner updates the plan of action and milestones to address vulnerabilities in the information system discovered during the assessment and to describe how the information owner/information system owner intends to address those vulnerabilities.

DRAFT

CONDUCT REMEDIATION ACTIVITIES

The information owner/information system owner should initiate remediation actions based on the findings produced during the assessment of the system's security controls, the outstanding items listed in the plan of action and milestones, and the results of performing the activities required by the system's security controls (e.g., vulnerability scanning, contingency plan testing, incident response handling). Security controls modified, enhanced, or added during this process should be reassessed by the assessor to ensure that appropriate corrective actions have been taken to eliminate previously identified weaknesses or deficiencies or to mitigate the previously identified risk to the organization.



Initiate Remediation Activities

Remediation activities are defined during security impact analyses and while conducting the ongoing assessments of security controls. The information owner/information system owner, in consultation with the authorizing official, senior agency information security officer, and risk executive (function), reviews each assessor finding and applies his or her judgment of the severity or seriousness of the finding and whether the finding is significant enough to be worthy of further investigation or remedial action. Senior leadership ensures that the organization's resources are effectively allocated in accordance with organizational priorities and provides resources first to the information systems that are supporting the most critical and sensitive missions for the organization or correcting the deficiencies that pose the greatest degree of risk.

For example, the information owner/information system owner in consultation with designated organizational officials may decide that certain assessment findings marked as *other than satisfied* are of an inconsequential nature and present no significant risk to the organization. Alternatively, the information owner/information system owner and organizational officials may decide that certain findings marked as *other than satisfied* are significant, requiring immediate remediation actions.

After the need for remedial action is confirmed by the authorizing official, the information owner/information system owner determines the appropriate steps required to correct any identified weaknesses and deficiencies. Any changes to the information system should be submitted for approval through the formal configuration management process.

Update Security Documentation

The information owner/information system owner updates the plan of action and milestones with any identified remedial actions planned for the information system along with the anticipated completion date for the activities. As the remediation activities are completed, the system security plan and plan of action and milestones is updated with the current system status.

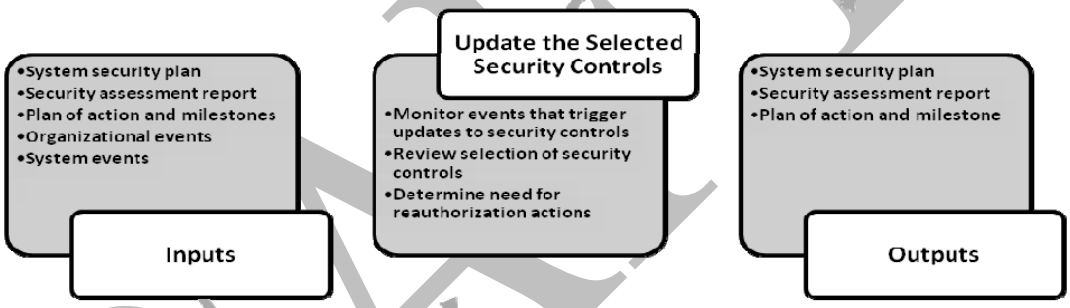
DRAFT

Assess System After Implementing Changes

After a change has been implemented in the information system, the information owner/ information system owner assesses the security controls of the system to determine if they remain effective.

UPDATE THE SELECTED SECURITY CONTROLS

Organizations should periodically determine if there is a need to update the current, agreed upon security controls documented in the security plan and implemented within the information system. Updating security controls may involve replacing a security control with a higher-impact level version of the control, adding a control enhancement, adding a new security control that was not included in the baseline that was selected for the system, or adding a compensating control or usage restriction. The information owner/information system owner needs to revisit, on a regular basis, the risk management activities described in the Risk Management Framework. Additionally, events such as security incidents, new legislation, or OMB policies may trigger the immediate need to assess the security state of the information system and require, if needed, an update of the selection of security controls.



Monitor Events that Trigger Updates to Security Controls

Events can occur that trigger the immediate need to assess the security state of an information system and, if required, to update the system's security controls. Examples of these events include:

- An incident results in a breach to an information systems that produces a loss of confidence in the confidentiality, integrity, or availability of the information processed, stored, or transmitted by the system;
- A newly identified, credible threat exists to the organization's operations, assets, or individuals (due to the use of the information system supporting those operations, assets, or individuals) based on law enforcement information, intelligence information, or other credible sources of threat information; or
- Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system.

Review Selection of Security Controls

When events such as those described above occur, the information owner/information system owner should review the security controls selected for the information system to determine if they remain sufficient to protect the information and information system assets against the newly identified vulnerabilities and threats. The information owner/ information system owner should reconfirm the system's impact level and security category of the information system and the information processed, stored, or transmitted by the system and determine if they need to be redetermined (following the guidance in

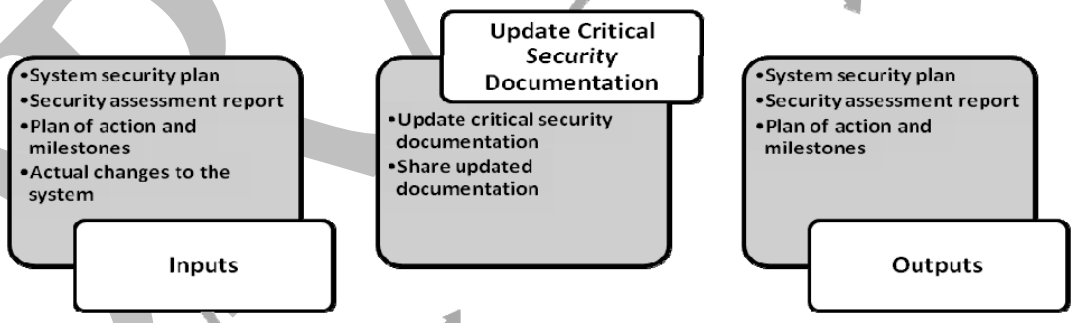
DRAFT

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*) and, if applicable, a higher or lower baseline set of security controls selected.

The organization should investigate the information system vulnerabilities exploited by the threat source (or that are potentially exploitable by a threat source) and the security controls currently implemented within the system (as described in the security plan). The exploitation of information system vulnerabilities by a threat source may be traced to one or more factors including but not limited to: (i) the failure of currently implemented security controls; (ii) missing security controls; (iii) insufficient strength of security controls; or (iv) an increase in the sophistication or capability of the threat source. Using the results from the assessment of the current security state, the information owner/ information system owner, with input from senior leaders (e.g., authorizing official, risk executive (function), senior agency information security officer) should reassess the risks to organizational operations, organizational assets, or individuals arising from use of the information system.

UPDATE CRITICAL SECURITY DOCUMENTATION

Continuous monitoring provides information owners/information system owners with an effective tool for producing ongoing updates to security plans, security assessment reports, and plans of action and milestones documents. The use of an automated support tool to allow authorizing officials and other senior leaders within the organization to obtain frequent security status information by examining the security plans for information systems, updated risk assessments, security assessment reports, and the plans of action and milestones documents is critical to understanding and explicitly accepting risk on a day-to-day basis.



Update Critical Security Documentation

The information owners/information system owners update the system security plan and the plan of actions and milestones to reflect changes in their information system while security assessors update the security assessment report with the results of the security control assessments. The frequency of updates to these critical security documents is at the discretion of the information owner/information system owner and the authorizing official in accordance with federal and organization policies. When updating the security documents, the information owner/information system owner should ensure that the past versions (including the original version) of the document are preserved and available for oversight, management, auditing, and security control assessment purposes.

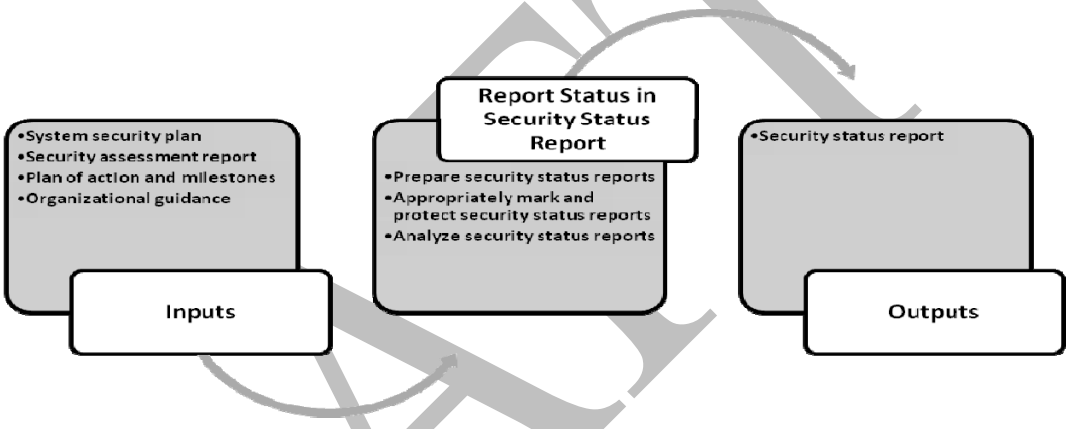
DRAFT

Share Updated Documentation

The information owner/information system owner should share the updated security documents with others, particularly with their interconnection partners. In the case of common controls, the common control provider should keep information owners/ information system owners informed about the level of security they are inheriting through the use of common controls in their individual information systems. In addition, the results of continuous monitoring should be reported to the authorizing officials, senior agency information security officer, and risk executive (function) on a regular basis so that they can determine the current security state of the information system, help manage risk, and provide essential information for reauthorization decisions.

REPORT STATUS IN SECURITY STATUS REPORTS

Information owners/information system owners should document the results of continuous monitoring activities in security status reports and provide them to the authorizing official and other designated senior leaders in the organization.



Prepare Security Status Reports

The security status reports should describe the continuous monitoring activities conducted during the reporting period, address the vulnerabilities discovered during the security control assessment or security impact analysis, and the information owner/ information system owner's plans to address those vulnerabilities. At a minimum, security status reports should summarize key changes to security plans (including risk assessments), security assessment reports, and plans of action and milestones. Security status reports should be appropriately marked, protected, and handled.

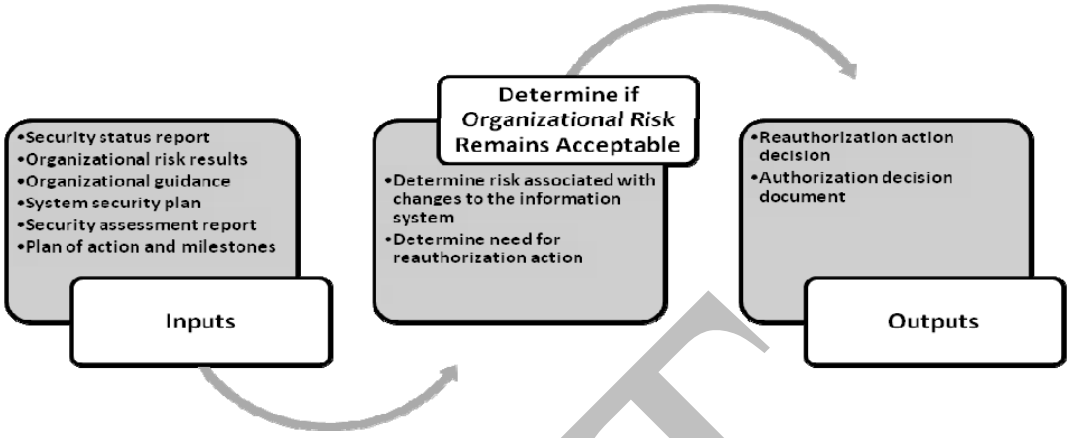
Analyze Security Status Reports

The information owner/information system owner should provide the security status reports at appropriate intervals to the authorizing official and other senior leaders to transmit significant security-related information about the information system but not so frequently as to generate unnecessary work.

DETERMINE IF RISK REMAINS ACCEPTABLE

The authorizing official may need to reauthorize an information system depending on the severity of an event, the impact of an event or change in the system on organizational operations, organizational assets, or individuals, and the extent of the corrective actions required to fix the identified deficiencies in the information system. The authorizing official makes the final determination on the need to reauthorize (for which an assessment of all of an information system's security controls is conducted) the information system in consultation with the information owner/information system owner, the senior agency information security officer, risk executive (function), and chief information officer. Continuous monitoring provides the information that the authorizing official needs to determine if reauthorization is required based on the current determination and acceptance of risk.

DRAFT



Determine Risk Associated with Changes to the Information System

The authorizing official reviews the security status reports to determine if the current risk of the information system to organizational operations and assets, individuals, other organizations, or the Nation remains acceptable and forwards appropriate direction to the information owner/information system owner. The information owner/information system owner should address the direction provided by the authorizing official to maintain the security status of the information system.

Determine Need for Reauthorization Action

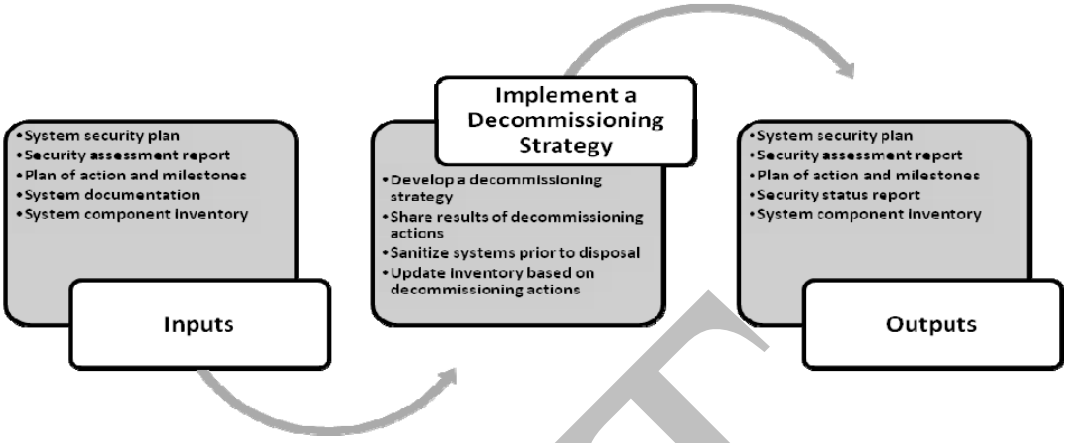
The authorizing official along with input from the senior agency information security officer and risk executive (function) should use the revised/updated security assessment report and the security status reports to determine if a reauthorization action is necessary. The continuous monitoring process provides the authorizing official and other organizational senior leaders with the information needed to determine the current security state of the information system, the resulting risk to the organization, and whether to allow continued operation of the system. The authorizing official should maintain sufficient knowledge of the current security state of the information system to determine whether continued operation is acceptable, and if not, which step of the Risk Management Framework needs to be executed in order to adequately mitigate the risk.

If the authorizing official determines that reauthorization is necessary, the authorizing official or designated representative documents the required actions in an authorization decision document that transmits an updated authorization decision to the information owner/information system owner and other key organizational officials. The authorization decision document identifies why reauthorization is needed, terms and conditions for the authorization including what steps within the Risk Management Framework should be completed, and the expected completion date for the reauthorization efforts.

IMPLEMENT A DECOMMISSIONING STRATEGY

When an information system is removed from operation, the information owner/ information system owner should ensure that all security controls addressing information system decommission (e.g., media sanitation, configuration management and control) are implemented.

DRAFT



Develop a Decommissioning Strategy

When an information system is no longer needed, the information owner/information system owner determines a strategy to decommission the system. The strategy should address the decommissioning roles and responsibilities and schedule, the reuse or disposition of system hardware, software, and firmware components, termination of contracts and other sharing arrangements, reuse, archival, or sanitization of system media, communication with system users, administrators, and managers, and updates of the organization's inventory.

Share Results of Decommissioning Actions

When information systems or information system components are decommissioned, users and application owners served by the decommissioned information system should be notified and any security control inheritance relationships should be reviewed and assessed for their security impacts.

Sanitize Systems Prior to Disposal or System Reuse

Sanitization is the process used to remove information from information system media so that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieve or reconstructed. Sanitation techniques, including clearing, purging, and destroying media information, prevent the disclosure of organization information to unauthorized individuals when the media is reused or disposed.

Update Inventory Based on Decommissioning Activities

The organization's tracking and management systems and the system security plan should be updated to indicate the specific information system components that are being removed from the system's inventory. When practical, automated mechanisms are used to maintain an up-to-date, complete, accurate, and readily available inventory of the information system components.

MONITOR STEP SUMMARY

A critical aspect of the security authorization process is the post-authorization period involving the continuous monitoring of an information system. Information from the continuous monitoring process is used to maintain a current understanding of the security state and risk posture of the organization and to facilitate appropriate risk mitigation actions. The information is also used to make credible, risk-based decisions regarding the continued operation of the organization's information systems, the continued use of common controls in the supporting infrastructure, and the explicit acceptance of risk that results from those decisions. Continuous monitoring processes also provide an organization with an effective tool for producing ongoing updates to security plans, security assessment reports, and plans of action and milestone documents.

DRAFT

The inputs and outputs of the continuous monitoring process are documented in critical security documentation (e.g., system security plan, security assessment report, security status reports, and plan of action and milestones) and includes the following:

- Changes to the information, information system, and operating environment;
- Organizational threat and vulnerability information;
- Continuous monitoring strategy;
- Results of system change reviews/approvals;
- System change implementations;
- Security impact analysis results;
- Remediation/corrective actions;
- Security status reports;
- Other security documentation (e.g., documentation of periodic vulnerability scans); and
- An updated information system that has undergone continuous monitoring and changes as conditions warrant

REFERENCES

- NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, Second Public Draft, April 2008
- NIST SP 800-37, Revision 1, *Guide for the Security Authorization of Federal Information Systems: A Security Life Cycle Approach*, Initial Public Draft, August 2008
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, Initial Public Draft, February 2009
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008
- NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008
- NIST SP 800-CM, *Security Configuration Management*, Internal Draft, October 2008
- Monitor Step FAQs, www.csrc.nist.gov//groups/SMA/fisma/Risk-Management--Framework/monitor/index.html

DRAFT