STUDENT GUIDE
Risk Management Framework –
Step 6: Monitor Security Controls

Slide 1 - Risk Management Framework

Welcome to Risk Management Framework –Lesson 6 - RMF Step 6 Monitor Security Controls.

Once an authorization decision has been made, the information system must be monitored. This is also referred to as Continuous Monitoring because it advocates continuously monitoring the system or information environment for security-relevant events and configuration changes that negatively affect security posture.

Slide 2 - Objectives

By the end of this lesson you should be able to:

- Explain the importance of documenting system changes
- Understand the need for ongoing assessment, risk determination and remediation
- Describe how assessor results can be used
- Determine the required frequency for reassessment
- Explain why status reporting is necessary
- Be familiar with the information system removal and disposal process

Slide 3 - Sources

The authoritative sources listed here are to be used for Continuous Monitoring Guidance:

- DoDI 8510.01 dated March 2014 is the high level document that sets forth the policy stating RMF is to be used by DoD
- NIST Special Publication 800-37 is the Guide for Applying RMF to Federal Information Systems
- The RMF Knowledge Service at https://rmfks.osd.mil/rmf is the go-to source when working with RMF (CAC/PKI required)

In addition, DoD is adopting NIST 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" and is currently developing a DoD Strategy for Continuous Monitoring.

STUDENT GUIDE
Risk Management Framework –
Step 6: Monitor Security Controls

Slide 4 – Who Are The Players?

There are seven tasks that comprise step 6 of the RMF. The following personnel have varying levels of responsibilities throughout this step:

- **Primary Responsibility:** Information System Owner or Common Control Provider, Authorizing Official or their Designated Representative and Security Control Assessor
- **Supporting Roles:** Information Owner or Steward, Information System Security Manager (ISSM), Information System Security Officer (ISSO), Risk Executive Function, Senior Information Security Officer (SISO), and Information System Security Engineer (ISSE)

Slide 5 - Task 6-1 System and Environment Changes

Now let's take a closer look at Task 1 where we determine the security impact of proposed or actual changes to the information system and its environment of operation.

The Information System Owner or Common Control Provider has Primary Responsibility for this task, while the Risk Executive Function, Authorizing Official or their Designated Representative, SISO, Information Owner or Steward and ISSO have supporting roles.

Slide 6 - Task 6-1 Record Changes

Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the system resides and operates. A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program.

It's important to record any relevant information about specific changes to hardware, software, or firmware such as version or release numbers, descriptions of new or modified features/capabilities, and security implementation guidance. It is also important to record any changes to the environment of operation for the information system (for example, modifications to hosting networks and facilities, mission/business use of the system, threats), or changes to the organizational risk management strategy. The information system owner and common control provider use this information in assessing the potential security impact of the changes.

STUDENT GUIDE
Risk Management Framework –
Step 6: Monitor Security Controls

Slide 7 - Task 6-1 Assess Impact of Changes

Documenting proposed or actual changes to an information system or its environment of operation, and subsequently assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring and maintaining the security authorization over time.

Information system changes are generally not undertaken prior to assessing the security impact of such changes. Organizations are encouraged to maximize the use of automation when managing changes to the information system or its environment of operation. Security-relevant changes may impact the authorization. Automated tools can help assess and track changes. (Wait for confirmation of this change.)

Security impact analysis conducted by the organization, determines the extent to which proposed or actual changes to the information system or its environment of operation can affect or have affected the security state of the system. Changes to the information system or its environment of operation may affect the security controls currently in place (including system-specific, hybrid, and common controls), produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously.

Slide 8 - Task 6-1 Corrective Actions

If the results of the security impact analysis indicate that the proposed or actual change can affect or have affected the security state of the system, corrective actions are initiated and appropriate documents revised and updated (for example, security plan, Security Assessment Report or SAR, and plan of action and milestones). The Information System Owner or Common Control Provider consults with appropriate organizational officials/entities, such as the configuration control board, senior information security officer and information system security officer, prior to implementing any security-related changes to the information system or its environment of operation.

The Authorizing Official or their designated representative uses the revised and updated Security Assessment Report in collaboration with the Senior Information Security Officer and Risk Executive Function to determine if a formal reauthorization is necessary. Most routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program, thus supporting the concept of ongoing authorization and near real-time risk management.

STUDENT GUIDE
Risk Management Framework –
Step 6: Monitor Security Controls

Slide 9 - Task 6-1 Update Risk Assessment

Conducting security impact analysis is part of an ongoing assessment of risk. As risk assessments are updated and refined, organizations use the results to modify security plans based on the most recent threat and vulnerability information available. Updated risk assessments provide a foundation for prioritizing/planning risk processes. The Authorizing Official or their designated representative in collaboration with the Risk Executive Function confirms determinations of residual risk. The Authorizing Official is kept apprised of any significant changes to the organizational risk posture.

Slide 10 - Task 6-2 Ongoing Security Control Assessments

Now we'll take a closer look at Task 2 where we assess the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

The Security Control Assessor has primary responsibility for this task, while the Authorizing Official or their Designated Representative, Information System Owner or Common Control Provider, Information Owner or Steward, and ISSM have supporting roles.

Slide 11 - Task 6-2 Frequency of Monitoring

Subsequent to the initial authorization, which is during the continuous monitoring period, the organization assesses all security controls, including management, operational, and technical controls, employed within and inherited by the information system on an ongoing basis. The frequency of monitoring is based on the monitoring strategy developed by the Information System Owner or Common Control Provider and approved by the Authorizing Official and Senior Information Security Officer.

Slide 12 - Task 6-2 Assessors

For ongoing security control assessments, assessors have the required degree of independence as determined by the Authorizing Official. Security control assessments in support of initial and subsequent security authorizations are conducted by independent assessors. Assessor independence during continuous monitoring, although not mandated, introduces efficiencies into the process and allows for reuse of assessment results in support of ongoing authorization and when reauthorization is required.

Slide 13 - Task 6-2 Results

Organizations can use the current year's assessment results to meet the annual FISMA security control assessment requirement. To satisfy this requirement, organizations can draw upon the assessment results from any of the following sources, including, but not limited to:

- Security control assessments conducted as part of an information system authorization, ongoing authorization, or formal reauthorization, if required
- Continuous monitoring activities, or
- Testing and evaluation of the information system as part of the system development life cycle process or audit, provided that the testing, evaluation, or audit results are current, relevant to the determination of security control effectiveness, and obtained by assessors with the required degree of independence

Slide 14 - Task 6-2 Reuse of Assessments

Existing security assessment results are reused to the extent that they are still valid and supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a cost-effective, fully integrated security program capable of producing the needed evidence to determine the security status of the information system.

Please note that the use of automation to support security control assessments facilitates a greater frequency and volume of assessments for the organization.

Slide 15 - Task 6-3 Ongoing Remediation Actions

Task 6-3 has to do with conducting remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the Plan of Action and Milestones.

The Information System Owner or Common Control Provider has Primary Responsibility for this task, while the Authorizing Official or their Designated Representative, Information Owner or Steward, ISSO, ISSE and Security Control Assessor have supporting roles.

Slide 16 - Task 6-3 Assessment Information

The assessment information produced during continuous monitoring is provided to the Information System Owner and Common Control Provider in an updated Security Assessment Report. They then initiate remediation actions on outstanding items listed in the Plan of Actions and Milestones, and

findings produced during the ongoing monitoring of security controls. The Security Control Assessor may provide recommendations as to appropriate remediation actions.

Security controls that are modified, enhanced, or added during the continuous monitoring process are reassessed to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk.

Slide 17 - Task 6-4 Key Updates

In Task 6-4 we want to update the security plan, Security Assessment Report, and Plan of Action and Milestones based on the results of the continuous monitoring process. Be sure to apply strict configuration management and control procedures whenever applying updates.

The Information System Owner or Common Control Provider has Pprimary responsibility for this task, while the Information Owner or Steward and ISSO have supporting roles.

Slide 18 - Task 6-4 What is Updated?

To facilitate the near real-time management of risk associated with the operation and use of the information system, the organization updates the security plan, Security Assessment Report, and Plan of Action and Milestones on an ongoing basis.

- The updated security plan reflects any modifications to security controls based on risk mitigation activities carried out by the Information System Owner or Common Control Provider
- The updated Security Assessment Report reflects additional assessment activities carried out to determine security control effectiveness based on modifications to the security plan and deployed controls
- The updated Plan of Action and Milestones
    - Reports progress made on the current outstanding items listed in the plan
    - Addresses vulnerabilities discovered during the security impact analysis or security control monitoring, and
    - Describes how the Information System Owner or Common Control Provider intends to address those vulnerabilities

The information provided by those key updates helps to raise awareness of the current security state of the information system (and the common controls inherited by the system) thereby supporting the process of ongoing authorization and near real-time risk management.

Slide 19 - Task 6-4 Frequency of Updates

The frequency of updates to risk management-related information is at the discretion of the Information System Owner, Common Control Provider, and Authorizing Officials in accordance with federal and organizational policies. Updates to information regarding the security state of the information system (and common controls inherited by the system) are to be accurate and timely since the information provided influences ongoing security-related actions and decisions by Authorizing Officials and other senior leaders within the organization.

With the use of automated support tools and effective organization-wide security program management practices, Authorizing Officials are able to readily access the current security state of the information system including the ongoing effectiveness of system-specific, hybrid, and common controls. This facilitates near real-time management of risk to organizational operations and assets, individuals, other organizations, and the Nation, and provides essential information for continuous monitoring and ongoing authorization.

Slide 20 - Task 6-5 Security Status Reporting

For Task 6-5, it is important to report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the Authorizing Official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy. Security status reports can take whatever form the organization deems most appropriate.

The Information System Owner or Common Control Provider has primary responsibility for this task, while the ISSO has a supporting role.

Slide 21 - Task 6-5 Status Reports slide

The results of monitoring activities are reported to the Authorizing Official on an ongoing basis in accordance with the monitoring strategy. Security status reporting can be event-driven (for example, when the information system or its environment of operation changes or the system is compromised or breached), time- driven (for example, weekly, monthly, quarterly) or both event- and time-driven.

Security status reports

- Provide the Authorizing Official, and other senior leaders within the organization, essential information with regard to the security state of the information system including the effectiveness of deployed security controls

- Describe the ongoing monitoring activities employed by the Information System Owner or Common Control Provider
- Address vulnerabilities in the information system and its environment of operation discovered during the security control assessment, impact analysis, and monitoring, and
- Show how the Information System Owner or Common Control Provider intends to address those vulnerabilities

Slide 22 - Task 6-5 Report Criteria and Use

The frequency of security status reports is at the discretion of the organization and in accordance with federal and organizational policies. Status reports occur at appropriate intervals to transmit significant security-related information about the information system, including information regarding the ongoing effectiveness of security controls employed within and inherited by the system, but not so frequently as to generate unnecessary work.

The Authorizing Official uses the security status reports in collaboration with the SISO and Risk Executive Function to determine if a formal reauthorization action is necessary. Security status reports are appropriately marked, protected, and handled in accordance with federal and organizational policies. At the discretion of the organization, security status reports can be used to help satisfy FISMA reporting requirements for documenting remedial actions for any security-related weaknesses or deficiencies.

Please note that status reporting is intended to be ongoing, not to be interpreted as requiring the time, expense, and formality associated with the information provided for the initial ATO. Rather, the reporting is conducted in the most cost-effective manner consistent with achieving the reporting objectives.

Slide 23 - Task 6-6 Ongoing Risk Determination and Acceptance

Task 6-6 is where the Authorizing Official reviews the reported security status of the information system, including effectiveness of deployed security controls, on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.

The Authorizing Official has primary responsibility for this task, while the Authorizing Official Designated Representative, Risk Executive Function and SISO have supporting roles.

Slide 24 - Task 6-6 Risk Review

Risks being incurred may change over time based on the information provided in the reports. Therefore the Authorizing Official or their designated representative reviews the information system on an ongoing basis to assess risk. The Authorizing Official determines, with inputs as appropriate from others with supporting roles, whether the current risk is acceptable and forwards appropriate direction to the Information System Owner or Common Control Provider. The use of automated tools to capture, organize, quantify, visually display, and maintain security status information promotes near real-time risk management regarding the overall organizational risk posture. The use of metrics and dashboards increases the ability to make risk-based decisions by consolidating data and providing it to decision makers at different levels within the organization in an easy-to-understand format. Determining how changing conditions affect mission and business risks associated with the information system is essential for maintaining adequate security. By carrying out ongoing risk determination and risk acceptance, Authorizing Officials can maintain the security authorization over time. The Authorizing Official also conveys updated risk determination and acceptance results to the Risk Executive Function.

Slide 25 - Task 6-7 OMB Circular A-130, Appendix III

In accordance with Appendix III of OMB Circular A-130, systems must be reassessed and reauthorized once every 3 years. The results of an annual review or a major change in the cybersecurity posture at any time may also indicate the need for reassessment and reauthorization of the system.

Systems that have been evaluated as having a sufficiently robust system-level continuous monitoring program, as defined by emerging DoD continuous monitoring policy, may operate under a continuous reauthorization.

Also note that continuous monitoring does not replace the security authorization requirement, but rather, it is an enabler of ongoing authorization decisions.

Slide 26 - Task 6-7 Information System Removal and Disposal

Finally, Task 6-7 is where we implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service.

The Information System Owner has primary responsibility for this task, while the Risk Executive Function, Authorizing Official, Designated Representative, SISO, Information Owner or Steward and ISSO have supporting roles.

STUDENT GUIDE
Risk Management Framework –
Step 6: Monitor Security Controls

Slide 27 - Task 6-7 Decommissioning

When a federal information system is removed from operation, a number of risk management- related actions are required.

- Organizations ensure that all security controls addressing information system removal and disposal (for example, media sanitization, configuration management and control) are implemented
- Organizational tracking and management systems (including inventory systems) are updated to indicate the specific information system components that are being removed from service
- Security status reports reflect the new status of the information system
- Users and application owners hosted on the decommissioned information system are notified as appropriate, and any security control inheritance relationships are reviewed and assessed for impact
- The effects of the subsystem removal or disposal are assessed with respect to the overall operation of the information system where the subsystem resided, or in the case of dynamic subsystems, the information systems where the subsystems were actively employed

Please note that this task also applies to subsystems that are removed from information systems or decommissioned.

Slide 28 - Milestone Checkpoint #6

This milestone checkpoint taken from NIST Special Publication 800-37 can be used to assess whether you are prepared to go to Step 6 of the RMF process.

Milestone checkpoints contain a series of questions for the organization to help ensure important activities have been completed(prior to proceeding to the next step.= may delete this phrase)

Slide 29 - Lesson Summary

In this lesson we discussed:

- The importance of documenting system changes
- The need for ongoing assessment, risk determination and remediation
- How assessor results can be used
- The required frequency for reassessment
- Why status reporting is necessary
- The information system removal and disposal process

Please click Next to complete the assessment questions in order to receive credit for this course.