RMF Stage 4 – Assessing Controls (Part One)

Reading

55m

✓ Status | Incomplete

Introduction

In the previous readings, you covered the first three stages of the RMF: *Categorize* (also known as Categorizing Systems), *Select* (also known as Selecting Controls), and *Implement* (Implementing Controls). In this reading, you will learn about the fourth and next stage of the RMF: *Assess*, also known as *Assessing Controls*.

More specifically, you will learn about the following topics:

- How to develop a security assessment plan
- How to assess controls as per the security assessment plan

Reading

How do you know systems are risk free? System security objective is met when:

- System is correctly characterized/categorized.
- Appropriate security controls are selected and tailored.
- Every applicable control is implemented or mitigated.
- Control assessment validates controls are correctly applied and effective.

At the **Assess** stage, you determine if the controls are in place, operating as intended, and producing the desired results. Assessment is the process of comparing actual and expected results; differences in the result represent residual risk. An assessment must be planned, documented, approved, and consistently applied. Also, it must be applied on a per-control basis.

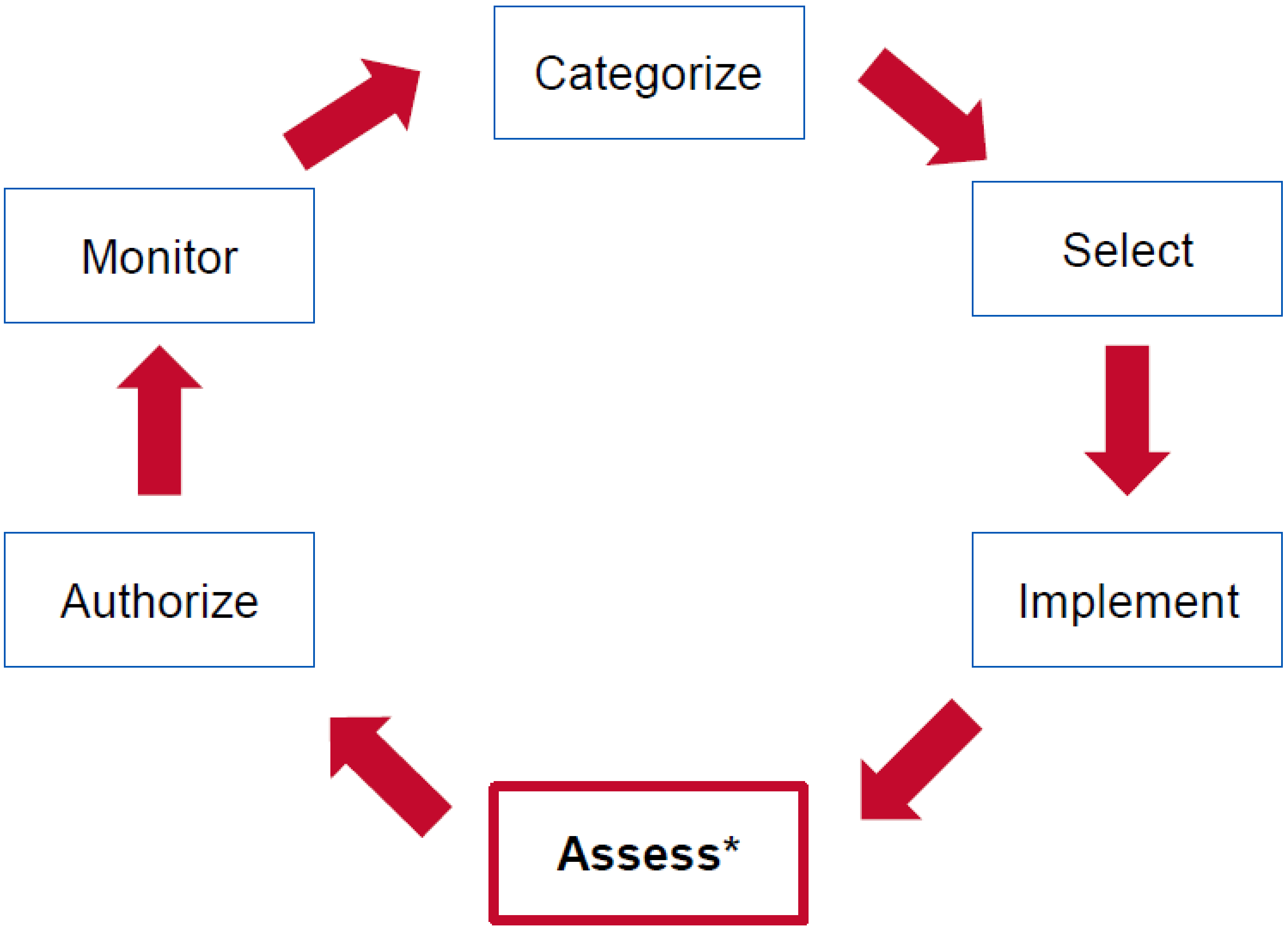


Figure 1: RMF – Assess (Source: NIST SP 800-37)

What is the Purpose of the Assess Step?

As explained by NIST, the purpose of the Assess step is to determine that selected security and privacy controls are implemented correctly, operate as intended, produce the desired outcome, and meet organizational or system security and privacy requirements. In the Assess step, the organization identifies control deficiencies and remediation actions. The Assess step tasks also describe assessor selection, assessment plan development, control assessments, assessment report development, and plan of action and milestones development and approval.

At the Assess stage, you complete four tasks:

1. Develop security assessment plan
2. Assess control compliance
3. Prepare security assessment report
4. Conduct remediation

In this reading, you will learn about the first two tasks of the Assess stage. The remaining two tasks will be covered in the next reading.

Task 1: Developing Security Assessment Plans

The **first task in the Assess stage** is to develop, review, and approve a plan to assess the security controls. The security assessment plan provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures.

The assessment plan reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions). Conducting security control assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions.

> **What Information do Assessment Plans Provide?**
>
> Assessment plans identify system, component, and organization-related roles and responsibilities, as well as assessment procedures for each security and privacy control. Assessment plans also identify the type of assessment to be conducted, such as development testing, initial authorization, re-authorization, or continuous monitoring.

Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security control assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the security authorization process to avoid system fielding delays or costly repetition of assessments.

The security assessment plan is reviewed and approved by appropriate organizational officials to ensure that the plan is consistent with the security objectives of the organization, employs state-of-the practice tools, techniques, procedures, and automation to support the concept of continuous monitoring and near real-time risk management, and is cost-effective with regard to the resources allocated for the assessment.

The purpose of the security assessment plan approval is two-fold:

1. To establish the appropriate expectations for the security control assessment.
2. To bound the level of effort for the security control assessment. An approved security assessment plan helps to ensure that an appropriate level of resources is applied toward determining security control effectiveness.

When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization obtains a security assessment plan from the provider.

Source: NIST

Technically Competent and Independent Assessors

Organizations consider both the *technical expertise* and *level of independence* required in selecting security control assessors. Organizations also ensure that security control assessors possess the required skills and technical expertise to successfully carry out assessments of system-specific, hybrid, and common controls. This includes knowledge of and experience with the specific hardware, software, and firmware components employed by the organization.

An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness.

Independent security control assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the assessor(s) conducting the assessment of the security controls.

The authorizing official or designated representative determines the required level of independence for security control assessors based on the results of the security categorization process for the information system and the ultimate risk to organizational operations and assets, individuals, other organizations, and the Nation. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to support a risk-based decision on whether to place the information system into operation or continue its operation.

Source: NIST

Control Coverage and Control Depth

Security assessment plans describe what controls will be assessed, including the coverage and depth of assessment, as explained below:

Control Coverage

- Assessment coverage depends on system familiarity (functionality and technology) and system impact.
- Control coverage can be comprehensive, focused, or basic:
    - Comprehensive coverage is when every control is assessed.
    - Focused coverage has a control subset based on criticality, familiarity, and threat environment.
    - Basic coverage is typically used in reauthorizations and is focused on system changes.

Control Depth

- Control coverage determines which controls are assessed while control depth determines how rigorously selected controls will be assessed
- In case of comprehensive coverage, there is rigorous assessment of every control requirement and every applicable control enhancement
- In case of focused coverage, the extent of assessment varies among controls and control enhancements.
- In case of basic coverage, there is superficial assessment of controls and enhancements.

Assessment Optimization

Assessment optimization determines the required level of independence. It is done in two steps:

Step 1: assessment sequencing has internal dependencies in case of control and control enhancements and external dependencies in case of related controls.

Step 2: assessment consolidation: * Merges related assessment requirements. * Performs after assessment sequencing. * Eliminates duplicative testing.

An example of assessment optimization is given below for your reference:

- **Control: AC-19 Access Controls for Portable and Mobile Devices**
    - Related controls:
        - MP-4 media storage
        - MP-5 media transport
    - Assessment of AC-19 depends upon results of MP-4, MP-5.
    - Assess MP-4, MP-5, AC-19 in order.
- **Controls: CM-2, CM-8, PL-2, RA-2, RA-3**
    - Considerable overlap in required information.
    - Consolidate questions.
    - Collect answers once.
    - Apply to all relevant controls.
- **Optimization driven by control baselines and overlays**
    - Document most common dependencies and consolidations.

Task 2: Conducting Security Controls Assessment

In the second task of the Assess stage, you assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

Control assessment guidance is generic and is not always a good fit for a specific system. Assessors are advised to consider the intent of the control. They should also consider the control context (system mission, operational environment, and unique organizational conditions).

In case of ISO 27008, auditors should:

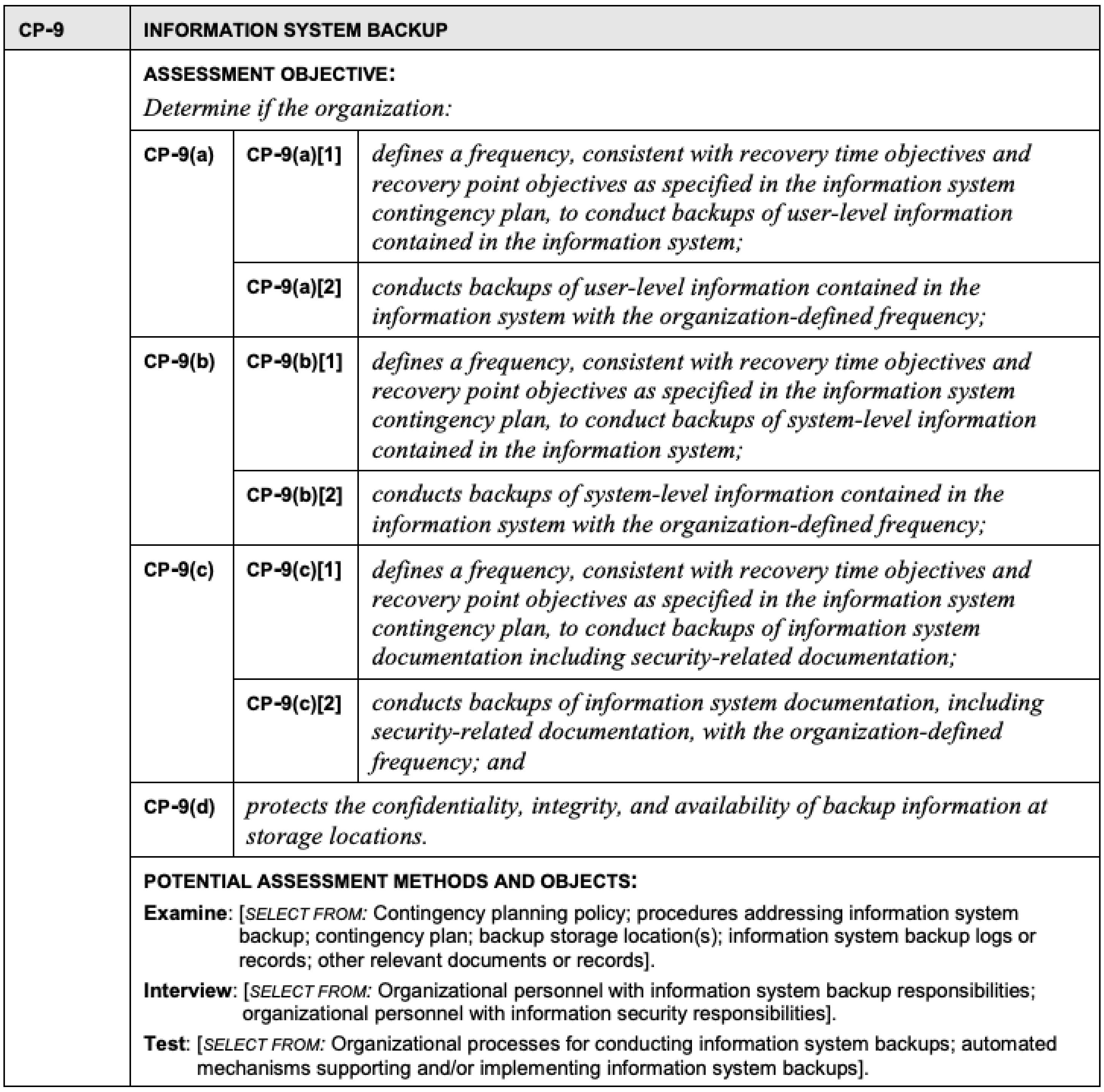
- Understand information system risks and security architectures.
- Be familiar with information security controls, practices, and standards.
- Be capable of examining complex technologies.
- Make practical application of information security reviews.

Assessment Procedures

As defined by NIST, an assessment procedure consists of a set of **assessment objectives**, each with an associated set of potential **assessment methods** and **assessment objects.**

An assessment objective includes a set of _determination statements _related to the particular security or privacy control under assessment. The determination statements are linked to the content of the security or privacy control (i.e., the security/privacy control functionality) to ensure traceability of assessment results back to the fundamental control requirements. The application of an assessment procedure to a security or privacy control produces assessment findings. These findings reflect, or are subsequently used, to help determine the overall effectiveness of the security or privacy control.

Assessment objectives are created for each control being validated; there is detailed guidance in NIST SP 800-53A. Also, they must be applied per the assessment plan.



CP-9	**INFORMATION SYSTEM BACKUP**		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	CP-9(a)	**CP-9(a)[1]**	*defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of user-level information contained in the information system;*
		CP-9(a)[2]	*conducts backups of user-level information contained in the information system with the organization-defined frequency;*
	CP-9(b)	**CP-9(b)[1]**	*defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of system-level information contained in the information system;*
		CP-9(b)[2]	*conducts backups of system-level information contained in the information system with the organization-defined frequency;*
	CP-9(c)	**CP-9(c)[1]**	*defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of information system documentation including security-related documentation;*
		CP-9(c)[2]	*conducts backups of information system documentation, including security-related documentation, with the organization-defined frequency; and*
	CP-9(d)	*protects the confidentiality, integrity, and availability of backup information at storage locations.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing information system backup; contingency plan; backup storage location(s); information system backup logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system backup responsibilities; organizational personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for conducting information system backups; automated mechanisms supporting and/or implementing information system backups].		

FIGURE 1: ASSESSMENT PROCEDURE FOR SECURITY CONTROL

Assessment Objectives

Assessment objectives define assessment object, assessment method, assessment coverage, assessment depth, and assessment findings, as explained below:

Assessment Object

Assessment objects identify the specific items being assessed and include *determination statements, specifications, mechanisms, activities, and individuals*, as explained below:

- Determination statements (qualities to be assessed)
- Specifications (documentary artifacts related to the control; plans, policies, procedures, regulations)
- Mechanisms (system functionality)
- Activities (actions to be taken in system configuration, operation, or sustainment)
- Individuals (parties responsible for performing activities)

Assessment Methods

Assessment methods define the nature of the assessor actions and include **examine**, **interview**, and **test**.

The **examine method** is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence.

The **interview method** is the process of holding discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence.

The **test method** is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior.

In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

> ℹ You will look at an example of assessment procedures (object, objectives, and methods) once you have covered the concept of assessment tailoring later in the reading.

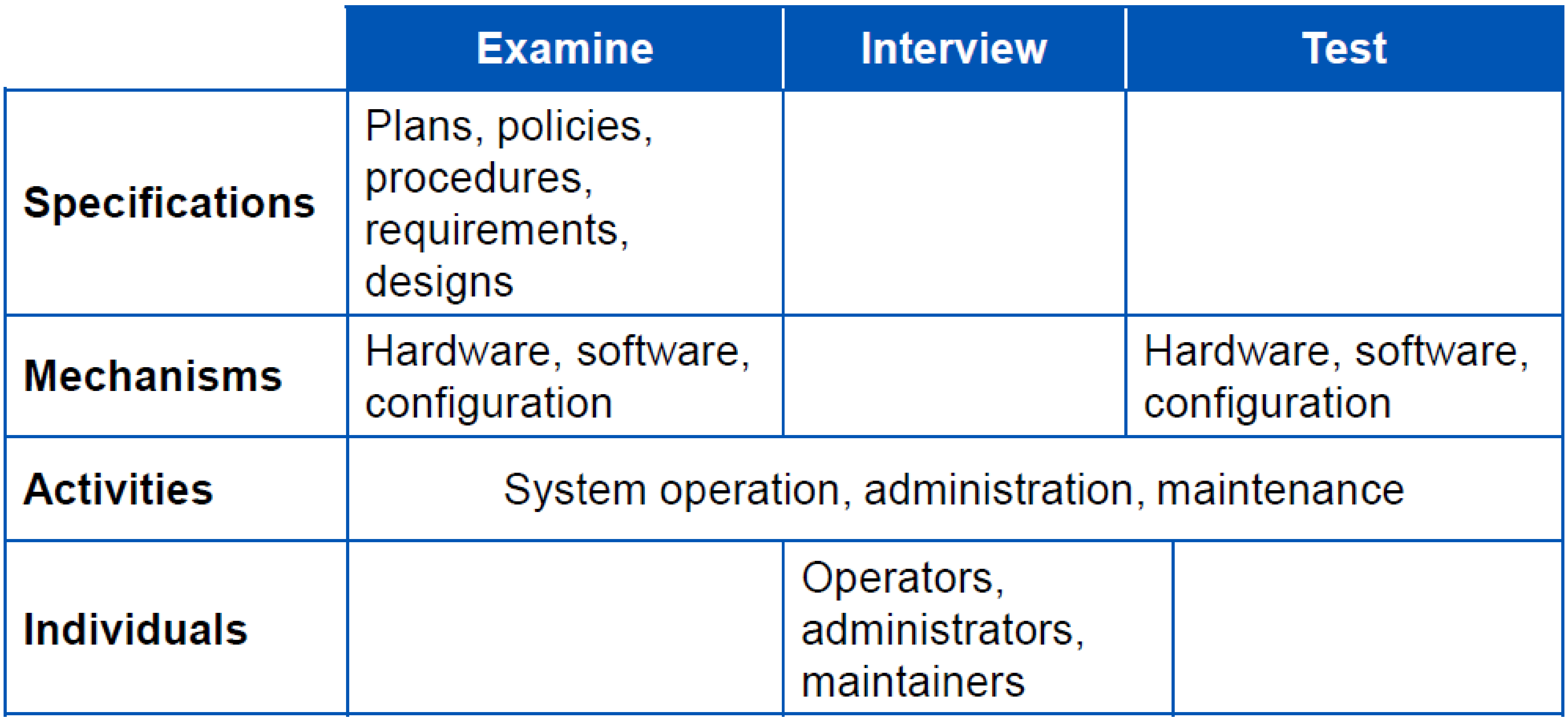
Testing Coverage and Depth

Assessment methods have a set of associated attributes, **depth,** and **coverage**, which help define the level of effort for the assessment. These attributes are hierarchical in nature, providing the means to define the rigor and scope of the assessment for the increased assurances that may be needed for some information systems.

The **depth attribute** addresses the rigor of and level of detail in the examination, interview, and testing processes. Values for the depth attribute include *basic*, *focused*, and *comprehensive*.

The **coverage attribute** addresses the scope or breadth of the examination, interview, and testing processes including the number and type of specifications, mechanisms, and activities to be examined or tested, and the number and types of individuals to be interviewed, as shown in the diagram below. Similar to the depth attribute, values for the coverage attribute include *basic*, *focused*, and _comprehensive. _

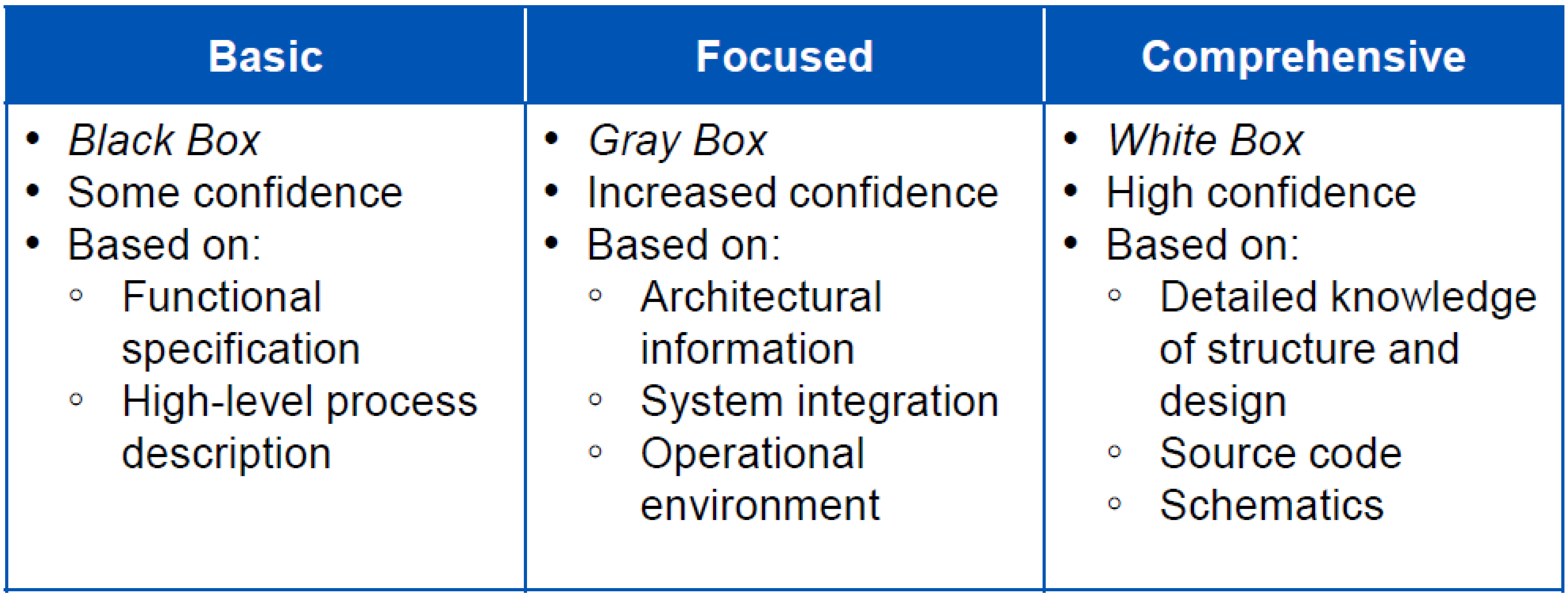
The appropriate depth and coverage attribute values for a particular assessment method are based on the assurance requirements specified by the organization. As assurance requirements increase with regard to the development, implementation, and operation of security and privacy controls within or inherited by the information system, the rigor and scope of the assessment activities (as reflected in the selection of assessment methods and objects and the assignment of depth and coverage attribute values) tend to increase as well.



	Examine	Interview	Test
Specifications	Plans, policies, procedures, requirements, designs		
Mechanisms	Hardware, software, configuration		Hardware, software, configuration
Activities	System operation, administration, maintenance		
Individuals		Operators, administrators, maintainers	

Table 1: Assessment methods: Examine, Interview and Test

Assessing Control Compliance



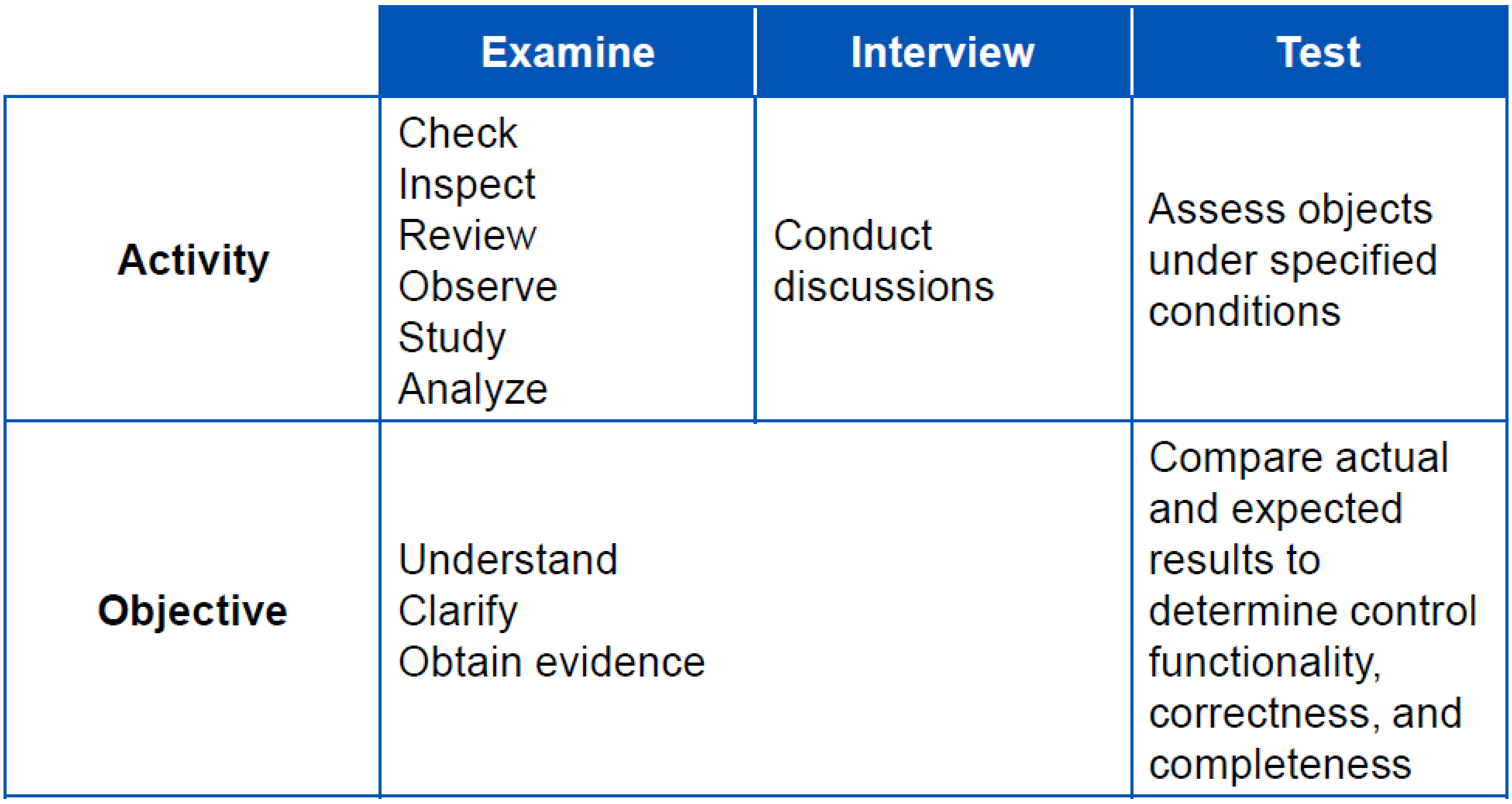
Basic	Focused	Comprehensive
• *Black Box* • Some confidence • Based on: ◦ Functional specification ◦ High-level process description	• *Gray Box* • Increased confidence • Based on: ◦ Architectural information ◦ System integration ◦ Operational environment	• *White Box* • High confidence • Based on: ◦ Detailed knowledge of structure and design ◦ Source code ◦ Schematics

Table 2: Assessing control compliance by leveraging Black Box, Gray Box, and White Box testing techniques

A comprehensive approach to assess the control compliance is by leveraging all three testing techniques: **Black Box**, **Gray Box**, and **White Box testing**. This will allow us to identify any gaps in coverage and depth of our control measures, as well as any vulnerabilities that may be present. Cyber Security professionals will review each test result to ensure that all controls are adequately compliant with the established policies and standards.

Black Box testing provides a view from an external perspective on how our controls measure up to industry standards and expectations. **Gray Box testing** is useful for uncovering gaps in security between two components, such as a firewall and an endpoint device. Lastly, **White Box testing** examines the code behind the system and evaluates the internal integrity of the security infrastructure. Through these comprehensive tests, we can ensure that our control measures are effectively mitigating risks while meeting industry compliance standards.

Assessment Activities



	Examine	Interview	Test
Activity	Check Inspect Review Observe Study Analyze	Conduct discussions	Assess objects under specified conditions
Objective	Understand Clarify Obtain evidence		Compare actual and expected results to determine control functionality, correctness, and completeness

Table 3: Assessment activities under Stage four Assessing Controls: Examine, Interview, and Test

Assessment activities refer to the methods used to evaluate the effectiveness of security controls implemented in a system. Under NIST SP 800-53 RMF Stage 4 - Assessing Controls, there are three assessment activities, Examine, Interview, and Test, as explained below:

- **Examine:** this activity involves reviewing documentation, policies, procedures, and other artifacts to determine if they are consistent with the security controls and requirements. This activity is primarily focused on assessing the control design.
- **Interview:** this activity involves conducting interviews with system administrators, security personnel, and other relevant stakeholders to verify that the controls are implemented and operating as intended. This activity is primarily focused on assessing the control implementation.
- **Test:** this activity involves testing the security controls to determine if they are effective in mitigating risks and protecting the system. This activity is primarily focused on assessing the control effectiveness.

To organize the assessment activities and objectives, a table can be used with assessment activities as the column headers and activities and objectives as the row headers. Here's an example:

Activities/Objectives	Examine	Interview	Test
Identify	x	x	x
Develop	x	x	x
Review	x	x	
Verify		x	x
Validate		x	x
Evaluate	x		x

Table 4: Organizing assessment activities and objectives in a table

In this table, the Activities/Objectives refer to the specific tasks or goals being evaluated, such as "Identify" for identifying security controls or "Develop" for developing security plans. The assessment activities are listed as the column headers and indicate which activity is being used to assess each objective. For example, "Examine" is used to assess “Identify”, “Develop”, “Review” and “Evaluate” objectives, while "Interview" is used to assess "Identify", "Develop", “Review”, "Verify" and “Validate”. Finally, the table indicates which objectives are being evaluated using each activity with an X in the appropriate cell.

Assessment Tailoring

In a manner similar to how the controls are tailored for the organization’s mission, business functions, characteristics of the system, and operating environment, organizations tailor the assessment procedures to meet specific organizational needs.

As you are aware, in the NIST SP 800-53 RMF, Stage 4 is the Assessing Controls stage. During this stage, an organization needs to assess the effectiveness of its security controls to ensure they are operating correctly and providing the necessary protection for the system and its data.

Assessment tailoring is the process of adjusting the level of rigor of the assessment based on the system's characteristics, the operating environment, and the specific requirements of the organization. It enables organizations to focus their assessment efforts on the most critical and relevant areas of the system.

To tailor the assessment, the organization needs to populate the parameters and adapt the generic objectives defined in the assessment procedures. Some examples of assessment tailoring include:

- **Populating parameters:** in the assessment procedures, there are specific parameters that need to be defined, such as the assessment boundary, the system environment, and the assessment objectives. These parameters need to be populated with specific information related to the system under assessment. For example, if the system under assessment is a cloud-based application, the assessment boundary would need to be adjusted to include the cloud environment.
- **Adapting generic objectives:** the assessment procedures define generic objectives that need to be achieved during the assessment. These objectives need to be adapted to fit the specific system and organization's requirements. For example, if the system under assessment stores sensitive information, the confidentiality objective would need to be adapted to ensure that the system adequately protects that information.
- **Adjusting assessment methods:** the assessment methods defined in the procedures may not be appropriate for all systems or organizations. Therefore, the assessment team needs to adjust the assessment methods to fit the specific system and organization's needs. For example, if the system under assessment is a legacy system, the assessment team may need to use manual testing methods instead of automated tools.

Assessment tailoring is an essential part of the RMF process as it allows organizations to focus their assessment efforts on the most critical areas of the system and ensure that the assessment is relevant and effective.

> Given below is a sample assessment object and corresponding assessment methods and objectives for your reference.

Assessment Object: Network Access Control (NAC)

Description: NAC controls ensure that only authorized devices and users can access the network.

Assessment Methods:

1. Penetration testing: the assessment team will attempt to bypass the NAC controls to gain unauthorized access to the network.
2. Configuration review: the assessment team will review the NAC configuration to ensure it aligns with the organization's security policies and industry best practices.
3. Compliance assessment: the assessment team will check the NAC controls against relevant regulations and standards, such as PCI-DSS or HIPAA.

Assessment Objectives:

1. Verify that the NAC controls are effective in preventing unauthorized access to the network.
2. Ensure that the NAC configuration aligns with the organization's security policies and industry best practices.
3. Confirm that the NAC controls meet relevant regulations and standards.

By tailoring the assessment methods and objectives to fit the specific NAC controls of the system, the organization can achieve a more effective and relevant assessment.

Key Takeaways

- The Assessing Controls stage is crucial to ensure the security controls are operating effectively and protecting the system and its data.
- Assessment tailoring is the process of adjusting the assessment methods and objectives to fit the specific system and organization's requirements.
- Populating parameters, adapting generic objectives, and adjusting assessment methods are some ways to tailor the assessment.
- The organization needs to define assessment objects, assessment methods, and assessment objectives to ensure a comprehensive and effective assessment.
- Assessment objectives should align with the organization's security policies, industry best practices, and relevant regulations and standards.
- Assessment results should be documented and reported to the organization's stakeholders to inform Risk Management decisions and improve the security posture.
- The Assessing Controls stage is iterative, and the organization needs to perform continuous monitoring and periodic reassessment to ensure the security controls remain effective over time.

Conclusion

In this reading, you looked at the first two tasks of the Assess RMF stage: *Developing Security Assessment Plan* and *Assessing Control Compliance*. In the next reading, Part Two, you will look at the next two tasks of this stage: *Preparing Security Assessment Report* and *Conducting Remediation*.

Further Readings

These resources provide detailed information and guidance on implementing the NIST SP 800-53 RMF process, conducting security assessments, and managing Cyber Security risks for organizations:

- NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations
- NIST Special Publication 800-53A, Revision 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations
- NIST Special Publication 800-37, Revision 2: Risk Management Framework for Information Systems and Organizations
- NIST Cybersecurity Framework
- NIST Privacy Framework

✓ Mark Completed

← Previous
Risk Management Methodology Document

Next
RMF Stage 4 – Assessing Controls (Part Two) →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W05D1

Mon Jul 22

› Lectures (1)

⌄ Work (8)

7 hrs

- </> Risk Management Methodology Document
- RMF Stage 4 – Assessing Controls (Part One)
- RMF Stage 4 – Assessing Controls (Part Two)
- ? GRC Quiz 2
- RMF Stage 5 - Authorizing Information Systems
- </> Conducting Residual Risk Assessment
- RMF Stage 6 - Monitoring Security Controls
- Writing Statement of Applicability (SOA)

W05D1 Schedule »

Powered by Lighthouse Labs.