RMF STEPS, TASKS, AND OUTCOMES PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://rmfstepstasksoutcomes.examzify.com

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. **Which outcome describes updating security and privacy plans to reflect control implementation changes made based on the assessments and remediation actions?**

   A. Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken.

   B. Security and privacy plans are updated to reflect control implementation changes made based on the assessments and remediation actions.

   C. A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed.

   D. Ongoing assessments of control effectiveness are conducted.

2. **How does RMF address changes to an information system after authorization?**

   A. Changes are assessed; may require updates to the SSP/POA&M and possibly a new authorization decision.

   B. Changes are ignored once authorized.

   C. Changes automatically revoke authorization.

   D. Changes require re-enrollment of all users.

3. **What is the purpose of the Security Assessment Report (SAR) in RMF?**

   A. To list deficiencies and remediation actions and tracks milestones.

   B. To define system boundaries and security responsibilities.

   C. To authorize system operation.

   D. To document the results of control testing, evidence, and overall control effectiveness.

4. **Which RMF artifact documents the security controls selected for a system and the plan for their implementation?**

   A. Project Charter

   B. System Security Plan (SSP)

   C. Incident Response Plan (IRP)

   D. Business Continuity Plan (BCP)

5. Which statement reflects independence in assessment?

A. An assessor or assessment team is selected to conduct the control assessments.

B. Independence is not considered in the selection.

C. The appropriate level of independence is achieved for the assessor or assessment team selected.

D. An assessor or assessment team is selected to conduct the control assessments and the appropriate level of independence is achieved.

6. Which artifact records the planned security assessment approach, scope, and procedures?

A. System Security Plan (SSP)

B. Security Assessment Plan (SAP)

C. Plan of Action and Milestones (POA&M)

D. Security Assessment Report (SAR)

7. Which outcome indicates developing and implementing a disposal strategy when appropriate?

A. The output of continuous monitoring activities is analyzed and responded to appropriately.

B. A system disposal strategy is developed and implemented, as needed.

C. A process to report the security and privacy posture to the authorizing official and other senior leaders and executives.

D. Risk management documents are updated based on continuous monitoring activities.

8. Which outcome involves identifying, documenting, and publishing common controls that can be inherited by organizational systems?

A. The organization-wide risk assessment is updated.

B. The types of information processed, stored, and transmitted by the system are identified.

C. Common controls that are available for inheritance by organizational systems are identified, documented, and published.

D. The authorization boundary is determined.

9. Who must approve compensating controls in RMF when a primary control cannot be implemented?

A. System Owner.

B. Authorizing Official.

C. Security Officer.

D. Project Manager.

10. What is the authorization package comprised of in RMF?

A. The SSP, SAR, risk assessment, POA&M, privacy considerations, and boundary documents.

B. The SSP and SAR only.

C. The risk assessment only.

D. Training records.

Answers

1. B
2. A
3. D
4. B
5. D
6. C
7. A
8. C
9. B
10. A

Explanations

1. Which outcome describes updating security and privacy plans to reflect control implementation changes made based on the assessments and remediation actions?

A. Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken.

B. Security and privacy plans are updated to reflect control implementation changes made based on the assessments and remediation actions.

C. A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed.

D. Ongoing assessments of control effectiveness are conducted.

Keeping security and privacy plans current after control changes is essential. When assessments identify gaps and remediation actions are implemented, updating the plans to reflect those control implementation changes ensures the documentation accurately mirrors the actual security posture. This alignment is crucial for ongoing authorizations, risk management, and clear accountability, so stakeholders and auditors see exactly what controls are in place, how they were changed, and why. Other options describe actions taken or documents used in the process, but they don't capture the step of updating the plans themselves to reflect the new control state.

2. How does RMF address changes to an information system after authorization?

A. Changes are assessed; may require updates to the SSP/POA&M and possibly a new authorization decision.

B. Changes are ignored once authorized.

C. Changes automatically revoke authorization.

D. Changes require re-enrollment of all users.

In RMF, once a system is authorized, it stays in a continuous monitoring state. When a change is made to the information system, you perform a security impact assessment to see if the change affects the security controls or the risk posture. If there is an impact, you update the System Security Plan to reflect the new controls or implementations and revise the Plan of Actions and Milestones with any remediation steps. Depending on how the change shifts risk, you may need a new authorization decision to allow operation under the updated risk level. Changes aren't ignored, they don't automatically revoke authorization, and they don't require re-enrolling all users.

3. What is the purpose of the Security Assessment Report (SAR) in RMF?

A. To list deficiencies and remediation actions and tracks milestones.

B. To define system boundaries and security responsibilities.

C. To authorize system operation.

D. To document the results of control testing, evidence, and overall control effectiveness.

In RMF, the Security Assessment Report captures the results of the security testing conducted on the system. It documents which controls were tested, how they were tested, the evidence collected, and an assessment of whether each control is effective and operating as intended. This provides the Authorizing Official with a clear view of the system's risk posture and residual risk, informing the authorization decision. The SAR is separate from the System Security Plan, which defines system boundaries and responsibilities, and from the Plan of Actions and Milestones, which tracks remediation actions. It isn't the authorization itself; it supports the decision by presenting the testing results, evidence, and overall control effectiveness.

4. Which RMF artifact documents the security controls selected for a system and the plan for their implementation?

A. Project Charter

B. System Security Plan (SSP)

C. Incident Response Plan (IRP)

D. Business Continuity Plan (BCP)

The System Security Plan (SSP) is the central RMF artifact that documents which security controls are selected for a system and describes how those controls will be implemented. It lays out the system boundary, the operating environment, and how the chosen controls meet security requirements. The SSP specifies the baseline controls, any tailoring, roles and responsibilities, and how the controls will be tested, assessed, and maintained over time. It also connects to the plan for ongoing risk management, often incorporating or referencing the plan of actions and milestones for addressing any gaps. This makes the SSP the key document used during authorization to explain what controls exist, how they're applied, and how the system will be operated securely. For contrast, a Project Charter focuses on project scope and objectives; an Incident Response Plan details how to detect and respond to security incidents; and a Business Continuity Plan outlines strategies to maintain operations during disruptions.

5. Which statement reflects independence in assessment?

A. An assessor or assessment team is selected to conduct the control assessments.

B. Independence is not considered in the selection.

C. The appropriate level of independence is achieved for the assessor or assessment team selected.

D. An assessor or assessment team is selected to conduct the control assessments and the appropriate level of independence is achieved.

Independence in assessment means the people conducting the evaluation are free from conflicts of interest and not involved in operating or managing the system being assessed, so their findings are objective and credible. The best choice reflects both the act of selecting someone to perform the control assessments and ensuring they have the appropriate level of independence. That combination ensures the assessment results can be trusted for risk decisions and authorization. Choosing only the assessor without guaranteeing independence leaves room for potential bias. Claiming independence isn't considered ignores a fundamental requirement for credible assessment. Holding independence without specifying the selection of an assessor leaves the process open to questions about who is evaluating and how they're chosen. The option that includes both selecting the assessor and achieving the right level of independence best captures how independence is integrated into the assessment process.

6. Which artifact records the planned security assessment approach, scope, and procedures?

A. System Security Plan (SSP)

B. Security Assessment Plan (SAP)

C. Plan of Action and Milestones (POA&M)

D. Security Assessment Report (SAR)

The key idea is identifying which artifact outlines how the security assessment will be conducted, including its overall approach, the system and controls to be assessed (scope), and the procedures to perform the assessment. The Security Assessment Plan does exactly that: it documents the methodology for evaluating security controls, defines the assessment scope and objectives, and lists the procedures, tools, roles, and schedule to carry out the assessment. It serves as the guide for how the assessment will be executed. In contrast, the System Security Plan describes the system and its security requirements and environment, providing context for controls but not the specific assessment plan. The Plan of Action and Milestones tracks remediation actions and timelines after findings are identified. The Security Assessment Report presents the results and findings of the assessment, not the plan for how the assessment will be conducted.

7. Which outcome indicates developing and implementing a disposal strategy when appropriate?

A. The output of continuous monitoring activities is analyzed and responded to appropriately.

B. A system disposal strategy is developed and implemented, as needed.

C. A process to report the security and privacy posture to the authorizing official and other senior leaders and executives.

D. Risk management documents are updated based on continuous monitoring activities.

Developing and implementing a disposal strategy when appropriate is about planning how and when to retire and securely destroy system components and data. The best outcome here is having a formal system disposal strategy created and put into action as needed, ensuring that assets are decommissioned safely, data is sanitized or destroyed properly, and any residual risks are addressed before disposal. This aligns with asset lifecycle management in RMF, where secure disposal protects information, supports compliance, and prevents data leakage. The other outcomes describe ongoing monitoring, governance reporting, and updating risk documentation based on monitoring results, which are important for ongoing risk management but do not focus on the disposal process itself.

8. Which outcome involves identifying, documenting, and publishing common controls that can be inherited by organizational systems?

A. The organization-wide risk assessment is updated.

B. The types of information processed, stored, and transmitted by the system are identified.

C. Common controls that are available for inheritance by organizational systems are identified, documented, and published.

D. The authorization boundary is determined.

Common controls are security measures that the organization implements at an organizational level and that can be inherited by individual systems. The outcome described focuses on identifying which of these controls exist, documenting them in a central catalog, and publishing them so system owners can rely on them during authorization. This reuse is powerful because it promotes consistency across many systems, reduces duplication of effort, and makes the assessment process more efficient since multiple systems can inherit the same set of controls rather than each building their own. Publishing the catalog ensures transparency and governability, so that when a system boundary is defined, the inherited controls are clearly identified and auditable. Other activities like updating risk assessments, identifying data processed by a system, or determining the authorization boundary do not specifically address the identification, documentation, and publication of common controls for inheritance.

9. Who must approve compensating controls in RMF when a primary control cannot be implemented?

A. System Owner.

B. Authorizing Official.

C. Security Officer.

D. Project Manager.

When a primary control can't be implemented, compensating controls are put in place to provide equivalent protection, and their approval is a formal risk acceptance decision. That approval comes from the person who has the authority to authorize operation of the system—the Authorizing Official. The AO reviews the security package, including the compensating controls and the residual risk, and decides whether to grant the Authorization to Operate. The System Owner is responsible for running the system and ensuring controls are in place, but cannot grant risk acceptance. The Security Officer handles implementation and ongoing security activities, not the authorization decision. The Project Manager oversees project delivery, not authorization. Because only the Authorizing Official has the authority to accept risk and authorize operation with compensating controls in place, they are the correct choice.

10. What is the authorization package comprised of in RMF?

A. The SSP, SAR, risk assessment, POA&M, privacy considerations, and boundary documents.

B. The SSP and SAR only.

C. The risk assessment only.

D. Training records.

In RMF, the authorization package is the collection of documents that show how the system's security controls are planned, tested, and managed, so an authorizing official can assess risk and make an authorization decision. The System Security Plan explains which security controls are in place and how they're implemented within the system. The Security Assessment Report captures the results of testing and evaluating those controls, including any weaknesses and their severity. The risk assessment analyzes overall risk to the system and its information, helping determine tolerable levels of risk. The Plan of Actions and Milestones records identified weaknesses and the remediation steps and timelines to address them. Privacy considerations ensure that handling of personal data complies with privacy requirements. Boundary documents define the system's scope, interfaces, and connections to other systems or networks. Training records, while important for personnel readiness, are not part of the authorization package.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://rmfstepstasksoutcomes.examzify.com

We wish you the very best on your exam journey. You've got this!