RMF Steps, Tasks, and Outcomes Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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 statement describes ongoing authorizations using the monitoring results and communicating changes in risk decisions and acceptance decisions?**

   A. **Risk management documents are updated based on continuous monitoring activities.**

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

   C. **Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.**

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

2. **What is a key outcome of Assessor Selection?**

   A. **An assessor is selected to conduct the control assessments.**

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

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

   D. **Assessors are selected after the assessment is complete.**

3. **Which outcome focuses on identifying, documenting, and publishing common controls available for inheritance 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.**

4. **Which outcome involves identifying and prioritizing stakeholder assets?**

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

   B. **The authorization boundary is determined.**

   C. **Mission/business processes identified.**

   D. **Stakeholder assets are identified and prioritized.**

5. What action is described by Update Control Implementation Information?

- **A. Documentation of planned control changes is optional.**
- **B. Changes to the planned implementation of controls are documented.**
- **C. The security and privacy plans are discarded after implementation.**
- **D. No changes are tracked.**

6. Which task covers Control Implementation?

- **A. Update Control Implementation Information**
- **B. Plan Review and Approval**
- **C. System Disposal**
- **D. Control Implementation**

7. What triggers a re-assessment or reauthorization in RMF?

- **A. Annual time-based requirement only**
- **B. Significant changes to the system after authorization**
- **C. Routine password changes**
- **D. New hardware only**

8. Documentation of planned control implementations is typically located in which documents?

- **A. Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.**
- **B. Controls are documented only in incident reports.**
- **C. Documentation is optional.**
- **D. Documentation is stored in a separate risk registry.**

9. What triggers a new authorization decision or reauthorization?

- **A. Minor system changes only**
- **B. Renewal interval only**
- **C. Re-scoping only**
- **D. Significant system changes, re-scoping, major incidents, or defined renewal interval**

10. Which task outcome requires reporting authorization decisions, significant vulnerabilities, and risks to organizational officials?

A. Security and privacy assessment reports are completed.

B. A plan of action and milestones is developed.

C. Risk determinations are rendered.

D. Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.

Answers

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

Explanations

1. Which statement describes ongoing authorizations using the monitoring results and communicating changes in risk decisions and acceptance decisions?

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

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

C. Authorizing officials conduct ongoing authorizations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.

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

Ongoing authorization rests on using continuous monitoring results to continuously reassess risk and keep authorization status up to date. The Authorizing Official uses those monitoring outputs to re-evaluate the system's risk posture and, when needed, adjust risk determinations and acceptance decisions. Crucially, this approach includes communicating any changes in risk determination and acceptance decisions to the right stakeholders, so everyone understands the current authorization status. The other ideas touch on related parts of the process—such as updating documents with monitoring findings or analyzing and reacting to monitoring outputs—but they don't capture the full action of the Authorizing Official conducting ongoing authorizations and explicitly communicating shifts in risk and acceptance decisions. System disposal strategy is unrelated to ongoing authorization.

2. What is a key outcome of Assessor Selection?

A. An assessor is selected to conduct the control assessments.

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

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

D. Assessors are selected after the assessment is complete.

The main idea is that an assessor or assessment team must be chosen to carry out the control assessments, and at the same time the level of independence they operate with must be appropriate for the task. This combination ensures the evaluations are objective and credible. When you select the right people to perform the assessments and also establish their independence from those who implement the controls, the results reflect reality rather than internal bias or pressure. Independence reduces conflicts of interest and supports unbiased judgment, while the right qualifications and role clarity ensure the controls are evaluated properly. If independence is considered without selecting who will perform the assessments, or if someone is chosen after the assessment is done, the process would lack objectivity and forethought.

3. Which outcome focuses on identifying, documenting, and publishing common controls available for inheritance 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.

Understanding how controls are managed across an organization is the heart of this concept. Common controls are security measures established at the organizational level that can be inherited by multiple systems within the organization. The key idea is to identify which controls exist, document them clearly, and publish them so that any system can reuse them without duplicating effort. This approach promotes consistency in security posture, reduces redundant work for individual systems, and provides a clear baseline for authorization processes. So, the best choice focuses on recognizing these organizational controls, recording them, and making them available for inheritance. Publishing them ensures system owners and assessors know what controls are in place and can rely on them during the authorization process. Other options relate to different activities: updating the organization-wide risk assessment addresses overall risk posture rather than the management and sharing of common controls; identifying the types of information a system processes concerns data inventory and classification; determining the authorization boundary deals with the scope of a system rather than how common controls are identified and reused.

4. Which outcome involves identifying and prioritizing stakeholder assets?

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

B. The authorization boundary is determined.

C. Mission/business processes identified.

D. Stakeholder assets are identified and prioritized.

Identifying and prioritizing stakeholder assets focuses the risk effort on what matters most to the organization and its stakeholders. It involves listing valuable items—data, systems, facilities, people, processes, and even reputation—and then ranking them by importance or criticality. This ensures that protective measures and resources are concentrated where they will have the greatest impact on mission success and risk reduction. By knowing which assets are most valuable, you can tailor controls and response plans to protect those assets effectively and allocate attention where it yields the biggest payoff. The other options cover related but different activities. Identifying the types of information processed, stored, and transmitted is about data classification, not prioritizing assets. Determining the authorization boundary defines the system's scope and perimeter, not which assets matter most. Identifying mission or business processes maps the organizational context, which is important but doesn't directly establish asset prioritization.

5. What action is described by Update Control Implementation Information?

A. Documentation of planned control changes is optional.

B. Changes to the planned implementation of controls are documented.

C. The security and privacy plans are discarded after implementation.

D. No changes are tracked.

Documenting changes to how controls will be implemented is about keeping an accurate, up-to-date record of how planned controls are actually deployed. In the RMF process, the plan for implementing security controls isn't fixed—deployment can lead to adjustments in baselines, control parameters, or the introduction of compensating measures. Recording these changes creates an auditable trail and ensures the security plan and assessment documentation reflect the current state, which in turn supports ongoing authorization and monitoring. If changes aren't documented, or if plans are discarded after implementation, or if no changes are tracked, the record would not reliably reflect reality or support subsequent evaluations.

6. Which task covers Control Implementation?

A. Update Control Implementation Information

B. Plan Review and Approval

C. System Disposal

D. Control Implementation

In RMF, putting security controls into operation is the action that directly realizes the chosen safeguards. The task that covers Control Implementation focuses on applying and configuring the selected controls across the system, documenting how each control is realized, and ensuring it's integrated with day-to-day operations. This is the phase where you actually enable protections—setting up access controls, encryption, monitoring, and system hardening so the controls function within the environment. The other options describe supporting or later activities: updating control implementation information is about maintaining documentation after deployment; plan review and approval is a governance step before deployment; and system disposal concerns decommissioning a system. So the task that best covers Control Implementation is the one that directly implements the controls.

7. What triggers a re-assessment or reauthorization in RMF?

A. Annual time-based requirement only

B. Significant changes to the system after authorization

C. Routine password changes

D. New hardware only

In RMF, ongoing monitoring ends with a decision about whether the authorization to operate remains valid. A reassessment or reauthorization is triggered whenever changes occur that could affect the system's security posture. The key driver is significant changes to the system after it has been authorized—such as substantial hardware or software updates, configuration changes, or changes in the operating environment—that could alter how well security controls work. Routine events like password changes are handled through day-to-day control updates and don't by themselves necessitate a full reassessment. Time-based schedule reviews may exist, but they don't replace the need to reassess when meaningful changes happen.

8. Documentation of planned control implementations is typically located in which documents?

A. Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.

B. Controls are documented only in incident reports.

C. Documentation is optional.

D. Documentation is stored in a separate risk registry.

Security and privacy plans or their equivalents are where the planned control implementations are captured. These documents specify which controls will be deployed, how they're tailored to the organization, who is responsible, and the timelines and methods for implementation, testing, and ongoing monitoring. They serve as the authoritative reference for how the organization intends to meet security and privacy requirements and show how those choices align with applicable frameworks and regulations. Incident reports focus on events after they occur, not planned controls. Documentation isn't optional in disciplined risk management, and while a risk registry may reference controls and treatments, it isn't the primary place to describe the planned implementations and tailoring.

9. What triggers a new authorization decision or reauthorization?

A. Minor system changes only

B. Renewal interval only

C. Re-scoping only

D. Significant system changes, re-scoping, major incidents, or defined renewal interval

In RMF, an authorization decision or reauthorization is prompted by changes that affect risk. Significant system changes can alter the security controls or the risk posture, requiring a fresh assessment. Re-scoping changes the system boundary and can reveal new risks or require different controls, so reevaluation is needed. Major incidents expose weaknesses that may shift risk levels, signaling the need to reassess. A defined renewal interval ensures periodic review and authorization, even if no other changes occur. The option that includes all these triggers—significant system changes, re-scoping, major incidents, or renewal intervals—best captures when a new authorization decision or reauthorization is warranted. The other choices are too narrow: minor changes alone don't typically drive a full reauthorization, renewal interval alone can miss changes between reviews, and re-scoping alone omits other triggers.

10. Which task outcome requires reporting authorization decisions, significant vulnerabilities, and risks to organizational officials?

A. Security and privacy assessment reports are completed.

B. A plan of action and milestones is developed.

C. Risk determinations are rendered.

D. Authorization decisions, significant vulnerabilities, and risks are reported to organizational officials.

The key idea here is governance through formal communication of risk and decision making. The task outcome that matches this is the one that explicitly requires reporting authorization decisions, significant vulnerabilities, and risks to organizational officials. This reporting ensures those responsible for oversight and risk management—the organizational officials—are informed of the authorization decision and the current risk posture, including any critical vulnerabilities that could affect the decision to operate the system. Security and privacy assessment reports collect and summarize findings from evaluations, but they don't by themselves convey the formal authorization decision or the ongoing risk status to governance so officials can act on it. A plan of action and milestones focuses on what actions will be taken and when, not on communicating the authority to operate or the broader risk context to officials. Risk determinations identify the level of risk, but without the explicit step of reporting those determinations and the related vulnerabilities to organizational officials, there's no formal governance channel to authorize or deny operation. So the best fit is the outcome that centers on reporting the authorization decision, vulnerabilities, and risks to those in charge of organizational governance. This ensures that the decision to authorize, require mitigations, or deny operation is made with full visibility at the leadership level.

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!