SPEA-V 369 – MANAGING INFORMATION TECHNOLOGY EXAM 1 PRACTICE (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://speav369managingit1.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 statement best describes least privilege in security?

A. Access rights are limited to the minimum necessary to perform tasks

B. All users have unlimited access to data

C. Access rights are granted randomly

D. Access rights require biometric verification for all actions

2. Which of the following is a pro of networking?

A. Mobility

B. Security Risks

C. Higher Costs

D. Installation More Disruptive

3. Which best distinguishes strategic and tactical planning?

A. Strategic: big picture; Tactical: how and who

B. Strategic: how; Tactical: big picture

C. Strategic: who; Tactical: what

D. Strategic: when; Tactical: where

4. Which sentence best defines risk in IT security?

A. A risk is something bad that could happen if threat happens because the vulnerability is exploited

B. A risk is the probability of a false positive

C. A risk is the time to recover from an incident

D. A risk is the cost of hardware

5. Which statement about training data is true?

A. It is used to train the model.

B. It is used to validate performance on unseen data.

C. It includes the correct labels for input data, guiding learning.

D. It is identical to testing data.

6. Why isn't open-source necessarily the lowest-cost option?

A. TCO analysis is required to determine this

B. Open-source is always cheaper

C. There are no costs for support

D. It cannot be used in enterprise

7. Shadow IT is best described as

A. IT offerings Not Provided By/Sanctioned by Business

B. IT services provided by the IT department only

C. IT services with formal governance

D. Shadow IT is a training program

8. What term describes informal, unsanctioned IT usage within an organization?

A. Shadow IT

B. End-State Solution

C. Operating System

D. Stakeholders

9. Which item is listed as a threat to IT systems today?

A. Insiders

B. Nation-State Actors

C. Botnets

D. Malicious Code

10. Which term describes a set of rules that govern how resources are accessed?

A. Encryption

B. Policy

C. Access Control

D. Authentication

Answers

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

Explanations

1. Which statement best describes least privilege in security?

A. Access rights are limited to the minimum necessary to perform tasks

B. All users have unlimited access to data

C. Access rights are granted randomly

D. Access rights require biometric verification for all actions

The key idea is that access should be limited to only what is necessary for a task. This minimizes the chances of accidental damage, reduces the impact of a compromised account, and makes security easier to manage. The description that access rights are limited to the minimum necessary to perform tasks captures this principle precisely. The other options stray from this idea: granting unlimited access ignores the protection framework; granting rights randomly undermines intentional control; and requiring biometric verification for all actions is a separate control, not the defining concept of least privilege.

2. Which of the following is a pro of networking?

A. Mobility

B. Security Risks

C. Higher Costs

D. Installation More Disruptive

Mobility is the key benefit of networking because it lets people stay connected and access shared resources from anywhere, using different devices. With a network, you can move between offices or rooms and still reach files, applications, printers, and cloud services without starting over, enabling roaming, remote access, and consistent authentication across devices. The other options point to challenges—security risks from more entry points, higher costs for infrastructure and maintenance, and potential disruption during setup—but they don't describe the advantages networking provides for staying connected as you move.

3. Which best distinguishes strategic and tactical planning?

A. Strategic: big picture; Tactical: how and who

B. Strategic: how; Tactical: big picture

C. Strategic: who; Tactical: what

D. Strategic: when; Tactical: where

Strategic planning focuses on the big picture and the long-term direction you want the organization to take. It sets overall goals, priorities, and where you want to be in the future. Tactical planning, on the other hand, breaks that direction into concrete steps: it decides how to implement the strategy, what specific actions to take, what methods to use, and who will carry them out. So the distinction is about scope and focus. Strategic is about the overarching goals and direction, while tactical is about the practical steps to achieve those goals and the people responsible for them. For example, a strategic aim might be to become a regional market leader in five years. The tactical plan would specify the projects, campaigns, resource allocations, timelines, and assignments needed to reach that aim. That's why describing strategic as the big picture and tactical as how to do things and who will do them best captures the fundamental difference.

4. Which sentence best defines risk in IT security?

A. A risk is something bad that could happen if threat happens because the vulnerability is exploited

B. A risk is the probability of a false positive

C. A risk is the time to recover from an incident

D. A risk is the cost of hardware

Risk in IT security is the potential for loss, damage, or disruption that could occur when a threat exploits a vulnerability. It reflects both how likely the harmful event is and how severe the impact would be, often framed as probability times impact. This matches the idea that risk is something bad that could happen if a threat takes advantage of a vulnerability. The other ideas describe different concepts: false positives relate to detecting benign events as threats; recovery time measures how long it takes to restore operations after an incident; and hardware cost concerns the price of equipment rather than the risk of harm from threats.

5. Which statement about training data is true?

A. It is used to train the model.

B. It is used to validate performance on unseen data.

C. It includes the correct labels for input data, guiding learning.

D. It is identical to testing data.

In supervised learning, the training data provides input examples paired with their correct outputs (labels). Those labels tell the model what the true answer should be for each example, and the learning process uses them to compute errors and adjust the model's parameters. This labeling is what guides the model to learn the mapping from inputs to outputs, making the statement about including the correct labels the accurate description of training data. While training data is indeed used to train the model, the key distinction is that the labels drive learning directly. Validation or test data, on the other hand, are used to evaluate performance on unseen data, not to guide learning. And training data is not the same as testing data.

6. Why isn't open-source necessarily the lowest-cost option?

A. TCO analysis is required to determine this

B. Open-source is always cheaper

C. There are no costs for support

D. It cannot be used in enterprise

Open-source software isn't automatically the cheapest option because what matters is the total cost of ownership over time. A TCO analysis looks at all costs beyond the initial price: deployment and integration, customization, training for users and admins, ongoing maintenance and security updates, potential downtime, and the cost of any required professional support. Depending on the project, these factors can add up and exceed the savings from not paying a licensing fee. That's why evaluating total cost of ownership is needed to decide which option is cheaper in a given context. Elements like "open-source is always cheaper," or "there are no costs for support," aren't accurate—support, integration, and maintenance can still incur significant expenses, and open-source is indeed used successfully in enterprise environments.

7. Shadow IT is best described as

A. IT offerings Not Provided By/Sanctioned by Business

B. IT services provided by the IT department only

C. IT services with formal governance

D. Shadow IT is a training program

Shadow IT refers to technology solutions used within an organization without the formal involvement, approval, or provisioning of the official IT group. Teams and units often seek faster, more flexible tools to meet immediate needs, so they turn to unsanctioned apps, services, or devices. This is why it's described as IT offerings not provided by or sanctioned by the organization's IT function: the solutions operate outside the established governance and support framework. The other ideas describe IT that is officially managed, governed, or part of a training program, which doesn't capture the unapproved, off-book nature of shadow IT.

8. What term describes informal, unsanctioned IT usage within an organization?

A. Shadow IT

B. End-State Solution

C. Operating System

D. Stakeholders

This question focuses on Shadow IT—the informal, unsanctioned use of IT resources within an organization. It happens when employees turn to apps, cloud services, or devices not approved by IT to meet work needs, often for speed or convenience. This makes Shadow IT the correct term, because it explicitly describes the practice of using technology outside formal governance. End-State Solution refers to a planned final outcome, Operating System is the software that runs devices, and Stakeholders are people affected by IT decisions, none of which describe the phenomenon of unauthorized IT usage. Shadow IT introduces risks like security gaps, data leakage, and compliance issues, which is why organizations aim to manage it with governance and controls.

9. Which item is listed as a threat to IT systems today?

A. Insiders

B. Nation-State Actors

C. Botnets

D. Malicious Code

Threats to IT systems today come in many forms, and malicious code is a central danger. Malicious code refers to software designed to harm, steal data, or take control of devices. It includes viruses, worms, trojans, ransomware, spyware, and other malware. Because it can spread quickly across networks, evade basic defenses, and compromise data, confidentiality, and operations, it remains one of the most encountered threats across organizations. Attackers deploy it through phishing emails, drive-by downloads, infected software, or compromised supply chains, enabling broader attacks and lasting impact. While insiders pose risk due to legitimate access, and nation-state actors or botnets are real threats, malicious code is the mechanism that makes many of these threats possible, making it the most representative answer for threats to IT systems today.

10. Which term describes a set of rules that govern how resources are accessed?

A. Encryption

B. Policy

C. Access Control

D. Authentication

Policy defines the rules and guidelines that determine who may access which resources and under what conditions. This governance layer establishes permissions, constraints, and the overall approach to security, guiding how access decisions are made and ensuring consistency across the system. That's why it's the best fit for describing a set of rules that govern access to resources. Encryption protects data by turning it into unreadable form, not by specifying who can access resources. Authentication is about verifying identity, not detailing who may do what. Access control is the mechanism that enforces rights defined by policy, applying those rules to grant or deny access, but the rules themselves come from the policy.

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://speav369managingit1.examzify.com

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