Network Security (NETSEC) 2 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 policy element is discretionary?

A. Standards

B. Guidelines

C. Both A and B

D. Neither

2. Planning, protection, and response follow a fairly strict sequence from one stage to another.

A. True

B. False

C. Not sure

D. Unknown

3. Single-Loss Expectancy multiplied by the Annualized Probability of Occurrence yields which metric?

A. Expected per-event loss

B. Expected annual loss

C. Expected life-cycle loss

D. Expected per-event benefit

4. Which statement best describes the relationship between security and functionality?

A. Security tends to impede functionality.

B. Security tends to improve performance.

C. Security has no impact on usability.

D. Security always eliminates risk entirely.

5. Conducting stings on employees _____.

A. Raises awareness

B. Raises resentment

C. Both A and B

D. Neither A nor B

6. Remediation plans should cover every security gap identified.

A. True

B. False

C. Only if approved by management

D. Only for high-severity gaps

7. What term describes closing all routes of attack into an organization's systems?

A. Defense in depth

B. Comprehensive security

C. Total security

D. Access control

8. Policies should specify implementation in detail.

A. True

B. False

C. Not required

D. Should be outsourced

9. _____ are payments made by a supplier to a corporate buyer when a purchase is made.

A. Bribes

B. Kickbacks

C. Both A and B

D. Neither A nor B

10. A(n) _____ is a statement of what should be done under specific circumstances.

A. implementation control

B. policy

C. policy guidance document

D. procedure

Answers

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

Explanations

1. Which policy element is discretionary?

A. Standards

B. Guidelines

C. Both A and B

D. Neither

Discretion in policy elements comes from whether compliance is required or left to judgment. In security policy frameworks, standards establish mandatory requirements that must be followed, while guidelines are recommended practices that teams can choose to implement or adapt based on context, resources, and risk. This makes guidelines the discretionary element: they guide behavior without enforcing it. A standard might require MFA for remote access, which is a non-discretionary mandate; guidelines would suggest MFA as a best practice but not require it in every situation. Therefore, the discretionary element is guidelines.

2. Planning, protection, and response follow a fairly strict sequence from one stage to another.

A. True

B. False

C. Not sure

D. Unknown

False — these activities are not strictly sequential; they are iterative and often overlap. In real-world incident handling, planning and protective measures run continuously and are updated as threats are detected and analyzed. When an incident occurs, teams may adjust plans, strengthen protections, and proceed with containment, eradication, and recovery in cycles rather than a fixed, one-way order. Frameworks like the incident response lifecycle show stages such as preparation, detection/analysis, containment, eradication, recovery, and post-incident review, but emphasize returning to earlier activities as needed rather than following a rigid line.

3. Single-Loss Expectancy multiplied by the Annualized Probability of Occurrence yields which metric?

A. Expected per-event loss

B. Expected annual loss

C. Expected life-cycle loss

D. Expected per-event benefit

The key idea is turning a single incident's financial impact into an expected yearly loss by accounting for how often the incident occurs. Single-Loss Expectancy is the loss that results from one incident. Annualized Rate of Occurrence represents how many such incidents are expected in a year (the frequency). When you multiply these together, you get the Expected Annual Loss, which is the average amount of money you would expect to lose each year due to that risk. This is expressed as currency per year. So the product of SLE and ARO yields the annualized loss figure used in risk assessment. It's not just the loss from one event (that would be SLE alone), and it isn't a total life-cycle loss or a per-event benefit, which is why the correct metric is the expected annual loss.

4. Which statement best describes the relationship between security and functionality?

A. Security tends to impede functionality.

B. Security tends to improve performance.

C. Security has no impact on usability.

D. Security always eliminates risk entirely.

Security design involves balancing protection with usable functionality. Every extra security control—like multi-factor authentication, encryption, strict access rights, or detailed auditing—adds processing steps, potential delays, or additional complexity. That overhead can slow down workflows, make interactions less smooth, and create compatibility challenges, so security often impedes functionality. It's not that security never helps usability—when integrated well, it enables trusted features and reduces downtime from breaches—but the general relationship is a trade-off: more security can come at the cost of how smoothly the system operates. The other statements misrepresent this balance: security doesn't usually improve performance, it isn't without impact on usability, and it cannot eliminate risk entirely.

5. Conducting stings on employees _____.

A. Raises awareness

B. Raises resentment

C. Both A and B

D. Neither A nor B

Internal sting operations affect employee attitudes in two ways: they raise awareness of policies and real-world consequences, and they can also provoke resentment or a sense of being constantly watched. When a test or sting demonstrates how easy it is to violate a policy or underlines what behavior is expected, employees learn what compliance looks like and why rules exist. At the same time, the element of surveillance or catching people in the act can feel punitive or distrustful, which can sour morale. Because both effects can occur in the same scenario, the best choice is that both awareness is raised and resentment can be produced. To keep this productive, organizations should pair stings with clear communication, fair review, and constructive feedback aimed at training and policy improvement rather than punishment.

6. Remediation plans should cover every security gap identified.

A. True

B. False

C. Only if approved by management

D. Only for high-severity gaps

Addressing all gaps identified in a security assessment creates a clear, accountable path to reduce risk. A remediation plan isn't just about fixing the most obvious problems; it maps every identified gap to a concrete action, assigns an owner, sets a timeline, and defines how the fix will be validated. This completeness matters because leaving gaps untracked or unaddressed leaves risk lurking, undermines audits, and makes governance harder. Even when some gaps are lower risk or require more resources, the plan should still document them with appropriate prioritization, rationale for any delay, and, if necessary, formal risk acceptance. That way, progress is measurable, and nothing slips through the cracks. Reckoning only the high-severity issues or needing management approval for every item would create gaps in coverage and slow down risk reduction, which is why a plan covering every identified gap is the best approach.

7. What term describes closing all routes of attack into an organization's systems?

A. Defense in depth

B. Comprehensive security

C. Total security

D. Access control

Closing all routes of attack into an organization's systems is best described by an all-encompassing security approach. Comprehensive security captures the idea of protecting every surface and entry point—people, processes, technology, and physical environments—through a coordinated set of policies, controls, monitoring, and governance. It implies assessing and securing the entire attack surface, not just one aspect, and continuously improving defenses to reduce exposure. Access control focuses narrowly on who can access specific resources, which is only one piece of the puzzle. Defense in depth is a solid strategy that emphasizes layered defenses, but the term doesn't by itself denote closing every possible route; it's about multiple defenses at different layers. Total security is not a standard term with a precise meaning in security practice and can be vague.

8. Policies should specify implementation in detail.

A. True

B. False

C. Not required

D. Should be outsourced

Policies establish high-level rules and objectives for security; they define what must be achieved, not how to achieve it. The detailed steps, controls, and configurations that implement those rules belong in procedures and standards, which can be updated as technology and environments change. Keeping implementation details out of policy preserves flexibility, allows tailoring to different systems, and ensures governance can adapt without rewriting the policy. For example, a policy might state that data must be encrypted, but the specific algorithm, key length, and key management practices are defined in a standard or procedure. If policies tried to specify implementation in detail, they would become rigid, harder to maintain, and less portable across diverse environments. Outsourcing concerns who performs the tasks, not the level of detail in the policy, and stating that implementation is required or not is separate from whether the policy should describe the exact steps.

9. _____ are payments made by a supplier to a corporate buyer when a purchase is made.

A. Bribes

B. Kickbacks

C. Both A and B

D. Neither A nor B

Kickbacks are payments made by a supplier to a corporate buyer in exchange for awarding the purchase to that supplier. These illicit incentives are intended to influence the buyer's decision and often accompany or follow the sale, creating a conflict of interest and constituting procurement fraud. A bribe is a broader term for any payment intended to sway decision-making, but the scenario described—money exchanged in relation to a specific purchase—fits the specific pattern of a kickback, making it the best fit.

10. A(n) _____ is a statement of what should be done under specific circumstances.

A. implementation control

B. policy

C. policy guidance document

D. procedure

Policies define management's expectations about what should be done under certain circumstances. They are high-level statements that express intent and guide decisions and behavior across the organization, specifying when actions are required and who is responsible. A procedure, by contrast, lays out the exact steps to take to carry out those actions, often in a detailed, sequential format. A policy guidance document provides recommendations for implementing or interpreting policies but isn't the binding directive itself. An implementation control isn't the term used for this concept in typical security practice. For example, a policy might state that all remote access requires multifactor authentication; a procedure would describe the specific steps to enroll and use MFA, and a policy guidance document would offer best-practice recommendations for implementing MFA.

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://netsec2.examzify.com

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