INTERNAL AUDITING STANDARDS AND PRACTICES – CYBERSECURITY PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://internalauditingcybersec.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. In auditing, practical wisdom is associated with which term?

A. Phronesis — practical wisdom for specific situations

B. Theoretical knowledge only

C. Strict rule following

D. Financial acumen

2. Which IT general controls are most relevant to cybersecurity, and how should an auditor assess their design and operating effectiveness?

A. Physical security

B. None

C. Access controls, change management, configuration management, backup and recovery, and IT operations; assess design against policy and standards, test operating effectiveness via walkthroughs, evidence, and sampling, and verify compensating controls.

D. Password policies

3. The auditor's role in cybersecurity is to:

A. Provide independent assessment, validate controls, identify blind spots, and ensure accountability

B. Conduct penetration testing

C. Manage daily security operations

D. Implement security architectures

4. Which statement describes the Third Line's role in risk management?

A. Owns and manages risk.

B. Supports, monitors, provides frameworks.

C. Independent assurance to the board.

D. Manages day-to-day security operations.

5. How should periodic access reviews and attestations be conducted to maintain least privilege?

A. Involve IT staff only to review access rights.

B. Involve business owners, validate role alignment, remove excess privileges, document attestations, and monitor exception handling and remediation.

C. Conduct reviews only annually with no attestations.

D. Automatically remove all privileged access monthly.

6. What conflicts of interest could arise in cybersecurity audits and how should they be managed?

A. External consulting; hide.

B. Vendor relationships; accept.

C. Personal relationships, external consulting, vendor relationships; manage by disclosure, recusal from affected areas, and independent review when necessary.

D. No conflicts of interest exist.

7. Independence risk of advisory work can impair future assurance objectivity if safeguards are not in place. Which statement best reflects this risk?

A. May impair future assurance objectivity — safeguards required.

B. May enhance assurance objectivity — no safeguards needed.

C. Has no impact on assurance objectivity.

D. Only affects audits of financial statements.

8. What is Domain III's biggest change in internal audit governance?

A. Explicit responsibilities for the board and senior management.

B. Expanded IT auditing scope.

C. Increased number of audits per year.

D. Centralized reporting to the external regulator.

9. Which type of control includes incident response and backups?

A. Corrective Controls

B. Preventive Controls

C. Detective Controls

D. Administrative Controls

10. Which option is not one of the three primary cybersecurity control types described?

A. Physical Controls

B. Preventive Controls

C. Detective Controls

D. Corrective Controls

Answers

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

Explanations

1. In auditing, practical wisdom is associated with which term?

A. Phronesis — practical wisdom for specific situations

B. Theoretical knowledge only

C. Strict rule following

D. Financial acumen

The concept being tested is practical wisdom in auditing, which goes beyond knowing rules or numbers and focuses on knowing how to act well in real, specific situations. The term phronesis captures this readiness to apply judgment, experience, and ethical consideration to determine the best course of action given the details at hand. In auditing practice, this means using professional skepticism and contextual understanding to assess risks, interpret evidence, and decide on appropriate procedures or disclosures tailored to the particular entity and situation. It's not just about theoretical knowledge or rigidly following rules, and it isn't merely about financial numbers; it's about prudent, well-reasoned action in the face of uncertainty and complexity. The other options don't fit because theoretical knowledge alone lacks practical application, strict rule following ignores the need for discretionary judgment, and financial acumen centers on numbers rather than contextual decision-making and ethics.

2. Which IT general controls are most relevant to cybersecurity, and how should an auditor assess their design and operating effectiveness?

A. Physical security

B. None

C. Access controls, change management, configuration management, backup and recovery, and IT operations; assess design against policy and standards, test operating effectiveness via walkthroughs, evidence, and sampling, and verify compensating controls.

D. Password policies

Understanding IT general controls that underpin cybersecurity means focusing on the controls that create a secure operating environment for all information systems. The most relevant set includes access controls to prevent unauthorized use, change management to ensure only approved changes are made, configuration management to keep systems in secure, known baselines, backup and recovery to protect data availability, and IT operations to sustain monitoring, scheduling, and incident response. This combination covers the major ways cybersecurity risks can materialize—through improper access, untested or unauthorized changes, insecure configurations, data loss, or unaddressed operational weaknesses. When assessing design, look for documented policies and standards for each area and evidence that the controls are properly embedded in the organization's control environment. For operating effectiveness, examine real-world execution: walkthroughs of processes, evidence such as access reviews, change tickets, configuration baselines, backup and recovery logs, and incident records, plus sampling to confirm that procedures are consistently followed. If a primary control isn't fully in place, verify that compensating controls exist and are appropriate, and that they provide equivalent assurance. Physical security or password policies alone don't provide the same comprehensive protection as the full suite of IT general controls, which is why the broader set is the best answer.

3. The auditor's role in cybersecurity is to:

A. Provide independent assessment, validate controls, identify blind spots, and ensure accountability

B. Conduct penetration testing

C. Manage daily security operations

D. Implement security architectures

The auditor's role in cybersecurity is to provide independent assurance that controls are appropriately designed and operating effectively. This means evaluating whether the organization's security controls actually mitigate the identified risks, validating that controls exist and function as intended, and looking for blind spots or gaps that management may have missed. It also includes ensuring accountability—confirming clear roles, responsibilities, evidence of remediation, and governance processes that hold owners responsible for addressing findings. Penetration testing, by contrast, is a specialized activity aimed at actively finding and exploiting vulnerabilities, typically done by security testers rather than auditors. Managing daily security operations is the job of the security operations team who monitor, detect, and respond to threats. Implementing security architectures is design and engineering work; auditors may review and assess architectures for adequacy, but they don't implement them.

4. Which statement describes the Third Line's role in risk management?

A. Owns and manages risk.

B. Supports, monitors, provides frameworks.

C. Independent assurance to the board.

D. Manages day-to-day security operations.

In risk management, three lines of defense separate responsibilities. The third line provides independent assurance to the board that governance, risk management, and internal controls are working as intended. This means internal auditors assess the design and operating effectiveness of controls, report findings to the board or audit committee, and remain objective because they operate independently of management. They don't own or manage risk themselves, aren't responsible for day-to-day security operations, and aren't the ones setting frameworks—those roles belong to the first and second lines. So the statement that best fits is that the third line offers independent assurance to the board.

5. How should periodic access reviews and attestations be conducted to maintain least privilege?

A. Involve IT staff only to review access rights.

B. Involve business owners, validate role alignment, remove excess privileges, document attestations, and monitor exception handling and remediation.

C. Conduct reviews only annually with no attestations.

D. Automatically remove all privileged access monthly.

Maintaining least privilege relies on ongoing, collaborative access reviews where business owners are involved. Regularly validating that each user's access aligns with their current role helps ensure privileges aren't wider than needed. Removing excess privileges prevents drift as job duties evolve, while attestations provide formal, documented confirmation that access is appropriate and creates accountability. Monitoring how exceptions are handled and remediated keeps control over any deviations and ensures timely fixes. Involving only IT staff misses essential business context and ownership. Conducting reviews only annually without attestations misses timely validation and accountability, increasing the risk of undetected privilege creep. Automatically removing all privileged access monthly is disruptive and impractical for operations.

6. What conflicts of interest could arise in cybersecurity audits and how should they be managed?

A. External consulting; hide.

B. Vendor relationships; accept.

C. Personal relationships, external consulting, vendor relationships; manage by disclosure, recusal from affected areas, and independent review when necessary.

D. No conflicts of interest exist.

In cybersecurity audits, maintaining independence and objectivity is essential to produce credible results. Conflicts can arise when an auditor has personal relationships with stakeholders, engages in external consulting for organizations connected to the audit, or has vendor relationships with suppliers whose products are being evaluated. The best way to handle these situations is to disclose any potential or actual conflicts early, recuse from parts of the work where the conflict could influence judgment, and bring in independent review or oversight when needed. This approach protects audit integrity, prevents biased conclusions, and helps maintain trust with stakeholders and regulators. Hiding conflicts undermines trust, accepting vendor relationships without safeguards invites bias, and assuming no conflicts exist ignores practical realities that need management.

7. Independence risk of advisory work can impair future assurance objectivity if safeguards are not in place. Which statement best reflects this risk?

A. May impair future assurance objectivity — safeguards required.

B. May enhance assurance objectivity — no safeguards needed.

C. Has no impact on assurance objectivity.

D. Only affects audits of financial statements.

Independence and objectivity are essential for credible assurance work. When the same internal team provides advisory services, it creates threats to objectivity in future assurance engagements, such as familiarity, self-interest, or pressure to please management. If safeguards aren't in place, those threats can bias judgment or reduce skepticism, undermining the trustworthiness of subsequent assurance reports. Safeguards help keep objectivity intact by separating duties and oversight: clear policies on independence, governance review by the audit committee, rotating staff or roles, strict boundaries between advisory and assurance activities, and documented assessments of any potential conflicts. With these protections, the risk to future assurance objectivity is managed, making the engagement more reliable. The other options don't fit because they either ignore the risk, suggest there's no need for safeguards, or limit the impact to a narrow scope (financial statements only). In reality, advisory work can affect future assurance across engagements, unless appropriate safeguards are in place.

8. What is Domain III's biggest change in internal audit governance?

A. Explicit responsibilities for the board and senior management.

B. Expanded IT auditing scope.

C. Increased number of audits per year.

D. Centralized reporting to the external regulator.

The main idea here is that governance relies on clear ownership at the top. The biggest change in Domain III's approach to internal audit governance is to require explicit responsibilities for the board and senior management. This means clearly defining who owns what in governance, risk management, and internal control—who sets risk appetite, who approves policies, who ensures controls are effective, and who supervises the overall governance framework. When these duties are clearly stated, it strengthens accountability and ensures top-level oversight aligns with what internal audit does, making assurance and advisory work more relevant and impactful. Other options relate to how much or where internal audit works rather than who is responsible for governance. Expanding IT auditing scope changes the focus area of audits, not who owns governance. Increasing the number of audits per year affects workload, not governance structure. Centralizing reporting to an external regulator would undermine independence and is not how governance ownership is typically defined.

9. Which type of control includes incident response and backups?

A. Corrective Controls

B. Preventive Controls

C. Detective Controls

D. Administrative Controls

Corrective controls are actions aimed at restoring normal operations after a security incident or failure and reducing the impact of that event. Incident response plans guide how to detect, contain, eradicate, and recover from a breach, with the recovery and restoration steps restoring services to their normal state. Backups provide a way to restore data to a known-good point after data loss or corruption, enabling systems to resume functioning with minimal downtime. Together, these activities focus on recovery and restoration, which is the essence of corrective controls. Preventive controls aim to prevent incidents from occurring (like strong access controls or patching), detective controls focus on identifying incidents as they happen (like continuous monitoring and log analysis), and administrative controls cover governance, policies, and procedures. That's why incident response and backups fit the corrective category.

10. Which option is not one of the three primary cybersecurity control types described?

A. Physical Controls

B. Preventive Controls

C. Detective Controls

D. Corrective Controls

The main concept tested is the classification of cybersecurity controls into three primary types: preventive, detective, and corrective. These categories describe how security measures aim to stop incidents, identify when they occur, and restore operations after an incident. Physical controls fit into physical security rather than the cyber control taxonomy. They include things like doors, locks, badges, surveillance cameras, and secure facilities. While they reduce risk and can indirectly support cybersecurity (for example, by preventing tampering with hardware or limiting access to critical systems), they are not considered one of the three primary cybersecurity control types that focus specifically on cyber-related activities. Therefore, Physical Controls are not one of the main cyber control types described.

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://internalauditingcybersec.examzify.com

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