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

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 15

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. How many Domains, Principles, and Standards exist in the 2024 IPPF?

A. 5 Domains, 15 Principles, 52 Standards

B. 3 Domains, 9 Principles, 30 Standards

C. 4 Domains, 12 Principles, 40 Standards

D. 6 Domains, 18 Principles, 60 Standards

2. Which factors expand an organization's attack surface?

A. New systems, integrations, users, vendors.

B. Increased firewall rules.

C. More security training for staff.

D. Expanded data center footprint.

3. Which of the following is NOT a recommended component of patch management effectiveness assessment?

A. Patch inventory and timely deployment.

B. Testing in staging and rollback plans.

C. Evidence of vulnerability remediation.

D. Immediate production deployment without testing.

4. The objective of the auditor's role in cybersecurity is to:

A. Provide independent assessment

B. Manage daily security operations

C. Guarantee breaches will not occur

D. Operate the security operations center

5. What does the practitioner rule on confidentiality imply about 'off the record' material?

A. It must still be documented if material.

B. It can be destroyed after discussion.

C. It should be sealed and never disclosed again.

D. It is exempt from audit trails.

SAMPLE

6. How should third-party risk be rated for vendors based on criticality and exposure in a cyber audit?

A. Based only on supplier location.

B. Based on supplier price.

C. Use a risk rating model considering data sensitivity, access levels, operational impact, regulatory exposure; document residual risk and monitoring requirements.

D. Based on vendor years in business.

7. Which statement best describes a preventive control?

A. A preventive control is designed to stop incidents before they occur.

B. A preventive control detects incidents after they occur.

C. A preventive control fixes vulnerabilities post-exploitation.

D. A preventive control is only about physical security.

8. Which elements should be assessed when auditing configuration management across endpoints to support cybersecurity?

A. Baseline configurations, change controls, patching cadence, deviation tracking, secure images, and enforcement evidence.

B. Historical incident costs.

C. User personas and marketing alignment.

D. Network latency and bandwidth only.

9. What are Topical Requirements in this context?

A. Ad hoc guidelines.

B. Mandatory audit requirements for high-risk areas.

C. Optional best practices.

D. Industry standards.

10. 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.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How many Domains, Principles, and Standards exist in the 2024 IPPF?

A. 5 Domains, 15 Principles, 52 Standards

B. 3 Domains, 9 Principles, 30 Standards

C. 4 Domains, 12 Principles, 40 Standards

D. 6 Domains, 18 Principles, 60 Standards

In the IPPF, the framework is built around three elements: Domains, Principles, and Standards. The five Domains describe broad areas of internal auditing practice. The fifteen Principles express fundamental expectations that apply across all domains and activities. The fifty-two Standards provide the formal requirements and guidance that govern how internal auditing is conducted, including attribute and performance aspects and any necessary implementation guidance. The 2024 IPPF uses this exact configuration, so five domains, fifteen principles, and fifty-two standards is the structure you're matching. The other options don't align with the updated 2024 framework, which is why this set best reflects the current IPPF.

2. Which factors expand an organization's attack surface?

A. New systems, integrations, users, vendors.

B. Increased firewall rules.

C. More security training for staff.

D. Expanded data center footprint.

Expanding an organization's attack surface happens when you introduce new entry points and trust relationships: new systems, new integrations, more users, and more vendors. Each addition adds interfaces, data flows, and potential misconfigurations that an attacker could exploit, widening the ways someone could breach defenses. While increasing firewall rules can help block traffic, and security training aims to reduce risk, and a larger data center footprint may bring more devices to secure, the most direct driver of a broader attack surface in this context is the introduction of new systems, integrations, users, and vendors.

3. Which of the following is NOT a recommended component of patch management effectiveness assessment?

A. Patch inventory and timely deployment.

B. Testing in staging and rollback plans.

C. Evidence of vulnerability remediation.

D. Immediate production deployment without testing.

Assessing patch management effectiveness hinges on making sure patches are identified, tested, and deployed in a controlled, timely way, with clear evidence that the vulnerabilities have been remediated. Having a current patch inventory and deploying patches promptly helps ensure systems aren't exposed longer than necessary and that nothing slips through the cracks. Testing patches in a staging environment and having rollback plans are essential to validate that the patch won't break critical functionality and to provide a safe path to undo changes if issues arise. Evidence of vulnerability remediation shows that the fixes were actually implemented and tracked, closing the loop from detection to resolution. The option that is not recommended is deploying patches directly to production without any testing. Skipping testing removes a crucial safety net: you can't verify compatibility with existing applications, determine the patch's real impact, or confirm that the vulnerability is properly mitigated without introducing new problems. This approach increases the risk of outages, performance problems, or other unintended consequences, which defeats the purpose of a thoughtful, controlled patch management process. So, while inventory, timely deployment, staging testing with rollback options, and documented remediation evidence all support an effective patch program, immediate production deployment without testing is the element that undermines reliability and should be avoided.

SAMPLE

4. The objective of the auditor's role in cybersecurity is to:

A. Provide independent assessment

B. Manage daily security operations

C. Guarantee breaches will not occur

D. Operate the security operations center

Independence and objective assessment of cybersecurity controls is what the auditor's role centers on. An auditor evaluates whether the controls are appropriately designed and operating effectively to manage risk, gathers evidence, conducts tests, and communicates findings and recommendations to management and the board. This independent assessment provides reasonable assurance that governance, risk management, and control activities are functioning as intended. It is not about running daily security operations or preventing all breaches; those are operational responsibilities of the security team, and no program can guarantee zero breaches. The value lies in documenting control design, performance, gaps, and remediation actions, enabling informed decisions and ongoing improvement.

5. What does the practitioner rule on confidentiality imply about 'off the record' material?

A. It must still be documented if material.

B. It can be destroyed after discussion.

C. It should be sealed and never disclosed again.

D. It is exempt from audit trails.

Confidentiality in internal auditing requires that information is protected and used only for the audit, but it still must be captured in a controlled, auditable record. When material is discussed off the record, it does not disappear; it should be documented so there is a trace of the discussion, the context, and any actions taken, while still keeping sensitive content appropriately protected. This ensures accountability, supports the audit conclusions, and aligns with records retention and access controls. Why the other ideas don't fit: destroying material after a discussion would break the audit trail and violate policy about retaining evidence; sealing it and never disclosing again would block legitimate disclosures to authorized stakeholders; and saying it's exempt from audit trails contradicts the fundamental need to maintain documented evidence of the audit process.

6. How should third-party risk be rated for vendors based on criticality and exposure in a cyber audit?

A. Based only on supplier location.

B. Based on supplier price.

C. Use a risk rating model considering data sensitivity, access levels, operational impact, regulatory exposure; document residual risk and monitoring requirements.

D. Based on vendor years in business.

Assessing third-party risk in a cyber audit requires a risk rating that reflects how critical a vendor is to operations and how exposed they are to cyber threats. The best approach uses a structured model that weighs data sensitivity, the level of access the vendor has to systems or data, the potential operational impact if the vendor is compromised, and any regulatory or contractual exposure tied to their activities. It also requires documenting the residual risk after existing controls and laying out monitoring requirements and triggers for action. This approach captures both likelihood and impact, guiding controls, due diligence, and ongoing oversight. Relying on supplier location, price, or years in business does not reliably indicate cyber risk posture or necessary controls, so those factors don't provide a sound basis for risk scoring.

SAMPLE

7. Which statement best describes a preventive control?

A. A preventive control is designed to stop incidents before they occur.

B. A preventive control detects incidents after they occur.

C. A preventive control fixes vulnerabilities post-exploitation.

D. A preventive control is only about physical security.

Preventive controls are proactive measures designed to stop security incidents before they happen by reducing the chance that a threat can exploit a vulnerability. They create barriers and enforce policies so problems are prevented rather than discovered or repaired after the fact. Examples include multi-factor authentication, strict access controls, network segmentation, timely patching, secure coding practices, and ongoing security training. This is why the statement describing prevention as stopping incidents before they occur fits best. By contrast, detecting incidents after they happen points to detective controls, fixing vulnerabilities after exploitation describes corrective controls, and focusing only on physical security misses the wide range of preventive measures used across people, processes, and technology.

8. Which elements should be assessed when auditing configuration management across endpoints to support cybersecurity?

A. Baseline configurations, change controls, patching cadence, deviation tracking, secure images, and enforcement evidence.

B. Historical incident costs.

C. User personas and marketing alignment.

D. Network latency and bandwidth only.

Maintaining consistent, secure endpoint configurations hinges on establishing known-good baselines, rigorous change controls, regular patching, deviation tracking, secure images, and enforcement evidence. A baseline configuration provides the reference state that endpoints should match, making it possible to quickly spot any drift or tampering. Change controls ensure that any modification to a device's setup goes through an approved process, with records and the ability to roll back if needed, which is essential for traceability and accountability. Patching cadence keeps systems up to date with the latest security fixes, reducing exposure to known vulnerabilities. Deviation tracking continuously monitors for configurations that diverge from the baseline, enabling prompt investigation and remediation of unauthorized or accidental changes. Secure images ensure that new or rebuilt endpoints start from a trusted, hardened state, lowering the risk of introducing malware or misconfigurations. Enforcement evidence demonstrates that these controls are actually implemented and monitored, providing auditable proof to regulators and stakeholders that the organization maintains a controlled, defensible endpoint environment. Historically, costs alone don't address how endpoints are configured or controlled, so they don't fit for assessing configuration management. User personas and marketing alignment aren't related to endpoint security configurations. Network latency and bandwidth measure performance rather than how configurations are established or enforced.

SAMPLE

9. What are Topical Requirements in this context?

A. Ad hoc guidelines.

B. Mandatory audit requirements for high-risk areas.

C. Optional best practices.

D. Industry standards.

Topical requirements are the mandatory audit focus areas chosen because they carry high risk and regulatory or policy obligations. In a cybersecurity audit, this means certain topics must be tested and evaluated because weaknesses in them would have the greatest potential impact or because laws and standards require evidence of controls in those areas. The auditor uses risk assessment results to decide which topics are non negotiable for the current audit scope, then plans tests, collects evidence, and reports on those areas accordingly. For example, topics like privileged access management, data protection and encryption, incident response, and third party risk are commonly designated as topical requirements because failures in these areas pose significant risk. This makes topical requirements distinct from ad hoc guidelines, optional best practices, or broader industry standards, which don't specify the mandatory coverage areas for a given audit.

10. 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.

SAMPLE

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!

SAMPLE