ISACA IT Risk Fundamentals Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Table of Contents

Copyright **1**

Table of Contents **2**

Introduction **3**

How to Use This Guide **4**

Questions **5**

Answers **9**

Explanations **11**

Next Steps **17**

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 risk is a part of overall business risk associated with the use, ownership, operation, involvement, influence and adoption of I&T within an enterprise?**

   A. I&T operations and service delivery risk

   B. Market risk

   C. I&T-related risk

   D. Likelihood

2. **What is the term for a repository of the key attributes of potential and known IT risk issues?**

   A. IT risk register

   B. Preventive control

   C. Risk map

   D. Risk owner

3. **Which term describes the repository containing key attributes of IT risks such as name, description, owner, expected/actual frequency, potential/actual magnitude, and disposition?**

   A. Risk aggregated

   B. IT risk register

   C. Quantitative risk analysis

   D. Risk map

4. **Which term describes the risk that I&T investment fails to provide value commensurate with its cost or is otherwise excessive or wasteful, including the overall I&T investment portfolio?**

   A. Asset Value

   B. Project Ownership Risk

   C. Relevance Risk

   D. Investment (Or Expense) Risk

5. Which term is defined as a mandatory requirement or specification approved by a recognized external standards organization?

A. Threat

B. Standard

C. Policy

D. Procedure

6. Which process involves diagnosing the origins of events, which can be used for learning from errors and problems?

A. Root cause analysis

B. Business case

C. Penetration test

D. Continuous risk and control monitoring

7. Which risk level is the exposure without considering management actions such as controls?

A. Inherent risk

B. Residual risk

C. Current risk

D. IT-related incident

8. What are the activities and programs designed to return the enterprise to an acceptable condition called?

A. ROI

B. Countermeasure

C. Disaster recovery

D. Business continuity

9. Which term is a forward-looking signal used to prompt early mitigations before problems occur?

A. Lead risk indicator

B. Lag risk indicator

C. KPI

D. Risk register

10. Which concept is a mechanism that reduces risk?

A. Risk transfer

B. Risk acceptance

C. Risk mitigation

D. Safeguard

Answers

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

Explanations

1. Which risk is a part of overall business risk associated with the use, ownership, operation, involvement, influence and adoption of I&T within an enterprise?

A. I&T operations and service delivery risk

B. Market risk

C. I&T-related risk

D. Likelihood

The key idea is that IT-related risk sits within the broader spectrum of business risk. When an organization uses, owns, operates, influences, and adopts information and technology, anything that could hinder achieving objectives—from governance and security to data integrity and system availability—counts as IT-related risk. It is the broad category that captures all risks tied to how IT affects the enterprise's ability to succeed. In contrast, IT operations and service delivery risk is a more specific, narrower slice focused on how IT services are run day to day. Market risk concerns external conditions affecting financial or market performance, not IT adoption inside the organization. Likelihood is about probability, not a risk category itself.

2. What is the term for a repository of the key attributes of potential and known IT risk issues?

A. IT risk register

B. Preventive control

C. Risk map

D. Risk owner

The main idea here is that a risk register is a centralized place to store all the essential details about IT risk issues, both those that might happen and those already identified. This repository holds the key attributes of each risk, such as a description, category, likelihood, impact, and overall risk rating, along with who owns the risk, the controls in place, any planned mitigations, status, and target dates. By keeping this information together, teams can consistently track, compare, and prioritize risks, assign accountability, and monitor remediation efforts over time. This makes it the most practical and comprehensive tool for managing risk information in an IT context. In contrast, a preventive control is a type of measure aimed at stopping events from occurring, a risk map is a visual layout of risk levels across dimensions, and a risk owner is the person responsible for managing a risk. So the repository that captures all these attributes is the IT risk register.

3. Which term describes the repository containing key attributes of IT risks such as name, description, owner, expected/actual frequency, potential/actual magnitude, and disposition?

A. Risk aggregated

B. IT risk register

C. Quantitative risk analysis

D. Risk map

The IT risk register is the centralized repository for IT risk data. It is a structured store that captures each identified risk with attributes such as name, description, owner, expected and actual frequency, potential and actual magnitude, and disposition. This format supports ongoing monitoring, accountability, and reporting by making it easy to track how risks change over time, who is responsible, what treatments are planned or in place, and the current risk level. The other terms describe different concepts: a risk aggregated is just a collection or summary of risks, not the data store; quantitative risk analysis refers to a method for calculating numeric risk values; and a risk map is a visual representation of risk levels, not the data repository.

4. Which term describes the risk that I&T investment fails to provide value commensurate with its cost or is otherwise excessive or wasteful, including the overall I&T investment portfolio?

A. Asset Value

B. Project Ownership Risk

C. Relevance Risk

D. Investment (Or Expense) Risk

The main idea here is about whether IT investments truly pay off relative to what they cost, and whether the overall mix of initiatives ends up wasteful. Investment (or expense) risk focuses on value realization across the IT portfolio—the chance that spending fails to deliver expected benefits or delivers less value than planned, including cost overruns, misaligned investments, or unnecessary expenditures across multiple initiatives. It specifically addresses the economic viability of the entire set of IT investments, not just a single asset or project. Other risks touch on different concerns: asset value looks at the worth of individual assets themselves, relevance risk concerns whether investments align with strategic objectives, and project ownership risk is about governance and accountability for a project.

5. Which term is defined as a mandatory requirement or specification approved by a recognized external standards organization?

A. Threat

B. Standard

C. Policy

D. Procedure

Standards are formal documents created by recognized external bodies that establish mandatory requirements or specifications. They provide a benchmark that organizations use to ensure consistency, interoperability, and compliance. Because they are approved by an external authority, standards carry an official, obliged status, which is why they're described as mandatory when adopted or required by regulation, contract, or governance practices. In contrast, a threat is a potential cause of harm, a policy is an internal rule reflecting management's intent, and a procedure is the specific steps to carry out a task. While policies may reference external standards and procedures implement them, the term that best fits a mandatory, externally approved requirement is the standard.

6. Which process involves diagnosing the origins of events, which can be used for learning from errors and problems?

A. Root cause analysis

B. Business case

C. Penetration test

D. Continuous risk and control monitoring

Root cause analysis focuses on identifying the underlying causes of events, so organizations can learn from mistakes and prevent recurrence. In IT risk management, when an incident occurs, this approach digs beyond the surface symptoms to find what in processes, controls, or human factors allowed the event to happen, then guides targeted corrective actions. Techniques like the 5 Whys or fishbone diagrams help teams trace a problem back to its fundamental driver, enabling meaningful improvements and preventing similar issues in the future. The other options address different aims. A business case is about justifying a project's value and viability, not diagnosing why an incident occurred. A penetration test evaluates security by simulating attacks to reveal vulnerabilities, not the origins of a past event. Continuous risk and control monitoring focuses on ongoing oversight of risk posture and control performance, not the retrospective analysis of an individual error to inform learning and root fixes.

7. Which risk level is the exposure without considering management actions such as controls?

A. Inherent risk

B. Residual risk

C. Current risk

D. IT-related incident

Inherent risk is the exposure that exists before any controls or management actions are applied. It represents how severe the threat and vulnerability combination could be if no safeguards are in place, essentially the maximum risk inherent to the asset or process. The question asks for the risk level without considering controls, which matches this definition exactly. Residual risk is the remaining risk after you implement controls. Current risk typically refers to the risk level with the present controls in place. An IT-related incident is not a risk level—it's a possible event. So the best answer is inherent risk.

8. What are the activities and programs designed to return the enterprise to an acceptable condition called?

A. ROI

B. Countermeasure

C. Disaster recovery

D. Business continuity

Disaster recovery focuses on restoring IT capabilities and operations after an interruption to bring the enterprise back to an acceptable level of service. It involves the plans, procedures, backups, and recovery steps needed to recover critical systems, data, and networks within defined recovery objectives (RTO and RPO), often including switching to alternate sites or redundant infrastructure. While business continuity is broader and aims to keep essential business functions running during a disruption, disaster recovery is the component that specifically gets technology and data back online after the event. ROI is a financial metric and not about restoration, and a countermeasure is a general risk-reduction action rather than the process of restoring operations.

9. Which term is a forward-looking signal used to prompt early mitigations before problems occur?

A. Lead risk indicator

B. Lag risk indicator

C. KPI

D. Risk register

Lead risk indicators are forward-looking signals that prompt early mitigations before problems occur. They forecast where risk may materialize and trigger proactive actions, such as increasing monitoring, tightening controls, or addressing vulnerabilities before an incident happens. Lag risk indicators, in contrast, show outcomes after the event and don't help prevent issues. KPIs measure performance and aren't inherently risk signals, and a risk register is simply a log of identified risks and planned responses, not predictive signals.

10. Which concept is a mechanism that reduces risk?

A. Risk transfer

B. Risk acceptance

C. Risk mitigation

D. Safeguard

Safeguard is a concrete control or mechanism put in place to reduce risk by lowering how likely a threat can exploit a vulnerability or by limiting the impact if it occurs. It includes technical controls, physical protections, or administrative policies and procedures. This directly reduces risk by acting as a protective measure. Risk transfer moves the potential impact to another party (for example, via insurance) rather than reducing the risk itself. Risk acceptance means choosing not to take action to reduce risk. Risk mitigation is the overall process or strategy to lower risk, but a safeguard is the specific mechanism used to achieve that reduction.

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://isacaitriskfundementals.examzify.com

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