Risks and Controls Exam 2 Practice (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. What is a control objective?

A. A method to train employees on technology

B. A financial plan for allocating resources

C. A specific goal that a control aims to achieve, such as accuracy or completeness of data

D. A strategy for increasing consumer engagement

2. How often should a risk assessment be conducted?

A. Monthly, or as frequently as possible

B. At least annually, or when significant changes occur

C. Only during financial audits

D. Every five years to align with corporate strategy

3. The inside environment of a data center should include all the following EXCEPT?

A. Cable management system

B. Backup power supply

C. Fire response systems

D. Heated floors

4. Which method is frequently used to determine the likelihood and impact of risks?

A. Pareto Analysis

B. Cost-Benefit Analysis

C. Risk Matrix Analysis

D. Statistical Process Control

5. In polite tailgating, what action does the authorized user take?

A. Accidentally opens the door

B. Spoofs the identity

C. Holds the door open for the tailgater

D. Forces entry

6. What type of risks does legal risk typically include?

- **A. Financial market risks**
- **B. Reputational risks**
- **C. Regulatory compliance risks**
- **D. Operational risks**

7. What primary function does a risk management information system serve?

- **A. Facilitating social interactions among employees**
- **B. Managing risk data for assessment, reporting, and compliance**
- **C. Performing market research**
- **D. Streamlining payroll processes**

8. Which of the following describes the purpose of detective controls?

- **A. To minimize the cost of internal audits**
- **B. To identify incidents after they have occurred**
- **C. To create awareness about compliance requirements**
- **D. To prevent risks from being introduced**

9. Define operational risk.

- **A. Risk of loss resulting from market fluctuations**
- **B. The risk associated with the failure of a product**
- **C. The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events**
- **D. Risk incurred during financial audits**

10. Womping Wembley Corp. maintains three sets of backups, which are updated monthly, weekly, and daily. This approach illustrates what?

- **A. Checkpoint and restart approach**
- **B. RAID approach**
- **C. Redundant backups approach**
- **D. Storage area network SANs approach**

Answers

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

Explanations

1. What is a control objective?

A. A method to train employees on technology

B. A financial plan for allocating resources

C. A specific goal that a control aims to achieve, such as accuracy or completeness of data

D. A strategy for increasing consumer engagement

A control objective is defined as a specific goal that a control aims to achieve, such as ensuring the accuracy, completeness, and reliability of data. This concept is central to the implementation of controls within an organization, as it provides a clear target for what the control is intended to accomplish. For instance, controls may be designed to prevent data entry errors, ensure that financial reports are complete, or safeguard sensitive information. By establishing these objectives, organizations can measure the effectiveness of their controls and determine whether they are meeting their intended purpose, thereby contributing to overall risk management and compliance efforts. The other choices, while related to business functions, do not accurately describe a control objective. Training employees on technology, allocating financial resources, or strategies for consumer engagement are processes or strategies but do not encapsulate the specific aim of controls within a risk management framework.

2. How often should a risk assessment be conducted?

A. Monthly, or as frequently as possible

B. At least annually, or when significant changes occur

C. Only during financial audits

D. Every five years to align with corporate strategy

Conducting a risk assessment at least annually or when significant changes occur is vital for maintaining an organization's risk management strategy. This approach ensures that the organization regularly evaluates its risk environment and updates its controls as necessary, accommodating new risks that may emerge or changes in existing risks. An annual assessment establishes a consistent review cycle, which is essential in industries where regulations or market conditions frequently evolve. Furthermore, addressing significant changes — such as mergers, acquisitions, shifts in operational processes, or changes in technology — allows organizations to adapt their risk management strategies promptly to mitigate potential issues that could impact the organization's objectives. While frequent assessments may provide a comprehensive view of risks, the option of conducting them solely during financial audits limits their frequency, leaving the organization vulnerable to newly emerging risks outside of those audit periods. Similarly, conducting risk assessments every five years could result in outdated information, making it risky for the organization, as the dynamic nature of risks necessitates more regular evaluations.

3. The inside environment of a data center should include all the following EXCEPT?

A. Cable management system

B. Backup power supply

C. Fire response systems

D. Heated floors

In a data center, the inside environment is designed to support the reliability, security, and efficiency of critical IT operations. A cable management system, backup power supply, and fire response systems are fundamental components of this environment. A cable management system is essential for organizing and protecting the vast amounts of cabling necessary in data centers, which aids in both operational efficiency and safety by minimizing hazards related to tangled cables. A backup power supply is crucial for maintaining continuous operations during power outages, ensuring that servers and critical infrastructure remain operational and minimizing the risk of data loss or downtime. Fire response systems are integral for safety and protecting valuable equipment. They include measures like fire detection and suppression systems that safeguard against potential fire hazards, which can be catastrophic in a data center setting. In contrast, heated floors, while they may assist with comfort in certain environments, are not a requisite element of a data center's operational infrastructure. Instead of relying on heated floors for temperature control, data centers typically use cooling systems to manage heat generated by servers and other equipment. Therefore, heated floors do not align with the primary goals of a data center's internal environment, which focuses on operational reliability and safety.

4. Which method is frequently used to determine the likelihood and impact of risks?

A. Pareto Analysis

B. Cost-Benefit Analysis

C. Risk Matrix Analysis

D. Statistical Process Control

The correct answer is the method that employs a Risk Matrix Analysis to assess the likelihood and impact of various risks. This analytical tool allows organizations to visually represent risks by categorizing them based on two main criteria: the probability of their occurrence and the potential impact or severity of their effects on objectives. By plotting risks on a matrix, stakeholders can easily identify which risks pose the greatest threat and prioritize them for mitigation efforts accordingly. The matrix typically consists of different levels of likelihood (e.g., rare, unlikely, possible, likely, certain) on one axis, and varying levels of impact (e.g., insignificant, minor, moderate, major, catastrophic) on the other. This systematic assessment aids in strategic planning and resource allocation when it comes to risk management. In contrast, other methods such as Pareto Analysis focus on identifying the most significant factors contributing to a problem rather than assessing risk likelihood and impact directly. Cost-Benefit Analysis evaluates the economic feasibility of actions but doesn't inherently address risk parameters. Statistical Process Control is more centered on process improvement and quality control, and while it may relate to risk in terms of variability, it does not directly analyze risk likelihood and impact in the same context as Risk Matrix Analysis.

5. In polite tailgating, what action does the authorized user take?

A. Accidentally opens the door

B. Spoofs the identity

C. Holds the door open for the tailgater

D. Forces entry

In polite tailgating, the action taken by the authorized user is to hold the door open for the tailgater. This situation often occurs in environments where access control is in place, such as secure buildings or restricted areas. The authorized user, by holding the door open, inadvertently allows individuals who may not have authorization to gain entry by closely following them. This action can stem from a desire to be courteous or from a lack of awareness regarding the security risks involved. Such behavior demonstrates the human element in security protocols, where social interactions can compromise safety measures. By understanding this concept, individuals can be better trained to recognize the importance of maintaining access control without inadvertently enabling unauthorized entry.

6. What type of risks does legal risk typically include?

A. Financial market risks

B. Reputational risks

C. Regulatory compliance risks

D. Operational risks

Legal risk primarily involves risks associated with the possibility of facing legal actions, penalties, or financial losses due to non-compliance with laws and regulations or contractual obligations. Regulatory compliance risks fall squarely within this category, as they pertain specifically to the pressures and potential repercussions that arise from failing to adhere to legal standards set by governing bodies. This encompasses the risk of fines or other sanctions that an organization might encounter if it fails to meet legal requirements. The other types of risks mentioned do connect with legal issues in some cases but are not exclusively defined by legal factors. For example, financial market risks pertain to uncertainties and potential losses linked to financial instruments, which may be influenced by legal conditions but are not rooted in them. Similarly, reputational risks revolve around how stakeholders perceive an organization, which can certainly be impacted by legal issues but does not directly fall under legal risk itself. Operational risks involve risks arising from internal processes, systems, or failures, and while they can include legal challenges, they encompass a broader range of issues not confined to legal matters. In summary, regulatory compliance risks are a core component of legal risk, directly reflecting the responsibilities to adhere to laws and regulations, making it the correct choice.

7. What primary function does a risk management information system serve?

A. Facilitating social interactions among employees

B. Managing risk data for assessment, reporting, and compliance

C. Performing market research

D. Streamlining payroll processes

A risk management information system (RMIS) is specifically designed to manage risk-related data, which is crucial for organizations in assessing potential risks, reporting on those risks, and ensuring compliance with relevant laws and regulations. By aggregating and analyzing risk data, an RMIS enables an organization to make informed decisions regarding risk management strategies, improve risk mitigation processes, and track compliance with industry standards. This centralized system enhances the ability to respond to risks effectively and to report risks to stakeholders, thus playing a pivotal role in an organization's overall risk management strategy. The other options do not align with the primary function of a RMIS. Facilitating social interactions is more aligned with collaboration tools, performing market research relates to business intelligence and analytics, while streamlining payroll processes is the domain of human resources management systems. Therefore, the focus remains on the management of risk data as the core function of a risk management information system.

8. Which of the following describes the purpose of detective controls?

A. To minimize the cost of internal audits

B. To identify incidents after they have occurred

C. To create awareness about compliance requirements

D. To prevent risks from being introduced

The purpose of detective controls is best described as identifying incidents after they have occurred. Detective controls are designed to detect and report any undesirable events, such as security breaches, fraud, or compliance failures, allowing organizations to respond and mitigate any potential impact. By monitoring, analyzing, and reviewing processes and systems, these controls provide insights into whether things are functioning as intended and highlight any issues that may require attention. In contrast, other options serve different purposes. For example, minimizing the cost of internal audits relates to efficiency improvements rather than detection of incidents. Creating awareness about compliance requirements is more aligned with training and educational measures, focusing on preventing violations before they happen. Lastly, preventing risks from being introduced pertains to preventive controls, which aim to stop issues from occurring in the first place rather than identifying them post-event. Therefore, the correct description of detective controls focuses on their role in recognizing incidents after they happen, enabling organizations to respond appropriately.

9. Define operational risk.

A. Risk of loss resulting from market fluctuations

B. The risk associated with the failure of a product

C. The risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events

D. Risk incurred during financial audits

Operational risk is fundamentally concerned with the potential for loss that arises from deficiencies or failures in an organization's internal processes, systems, or people, as well as from external events. This broad definition encompasses a wide variety of potential issues, including, but not limited to, administrative errors, system failures, fraud, or external disruptions such as natural disasters. By focusing on "inadequate or failed internal processes, people, and systems or from external events," the definition captures the essence of operational risk as it relates to the overall functionality and reliability of an organization. It highlights that not only internal factors can lead to risk; external events also play a critical role in the operational risk landscape. This understanding is crucial for organizations in conducting risk assessments and implementing controls to mitigate potential losses arising from these myriad sources. By recognizing and defining operational risk in this manner, it allows for a more comprehensive risk management strategy that can address a wide range of possible failures and challenges.

10. Womping Wembley Corp. maintains three sets of backups, which are updated monthly, weekly, and daily. This approach illustrates what?

A. Checkpoint and restart approach

B. RAID approach

C. Redundant backups approach

D. Storage area network SANs approach

The correct choice reflects the concept of the Redundant backups approach because Womping Wembley Corp. is employing a strategy that maintains multiple sets of backups. By updating backups on different schedules—monthly, weekly, and daily—the corporation ensures that there are various restore points available. This redundancy is crucial for disaster recovery, as it allows the organization to recover data from the most recent backups if necessary. The rationale behind maintaining this redundancy is to mitigate the risk associated with data loss. Should the primary data become corrupted or lost, the organization can resort to one of the backup sets, thereby minimizing downtime and data loss. The other approaches listed do not incorporate the element of providing multiple, temporal points of data recovery in the same way this backup strategy does. For instance, the checkpoint and restart approach centers on the ability to return a system to a known good state rather than managing multiple backups over time. RAID focuses on data storage solutions that provide fault tolerance rather than backup frequency, while Storage Area Networks (SANs) refer to networked storage solutions rather than specific data recovery or backup strategies.

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://riskscontrols2.examzify.com

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