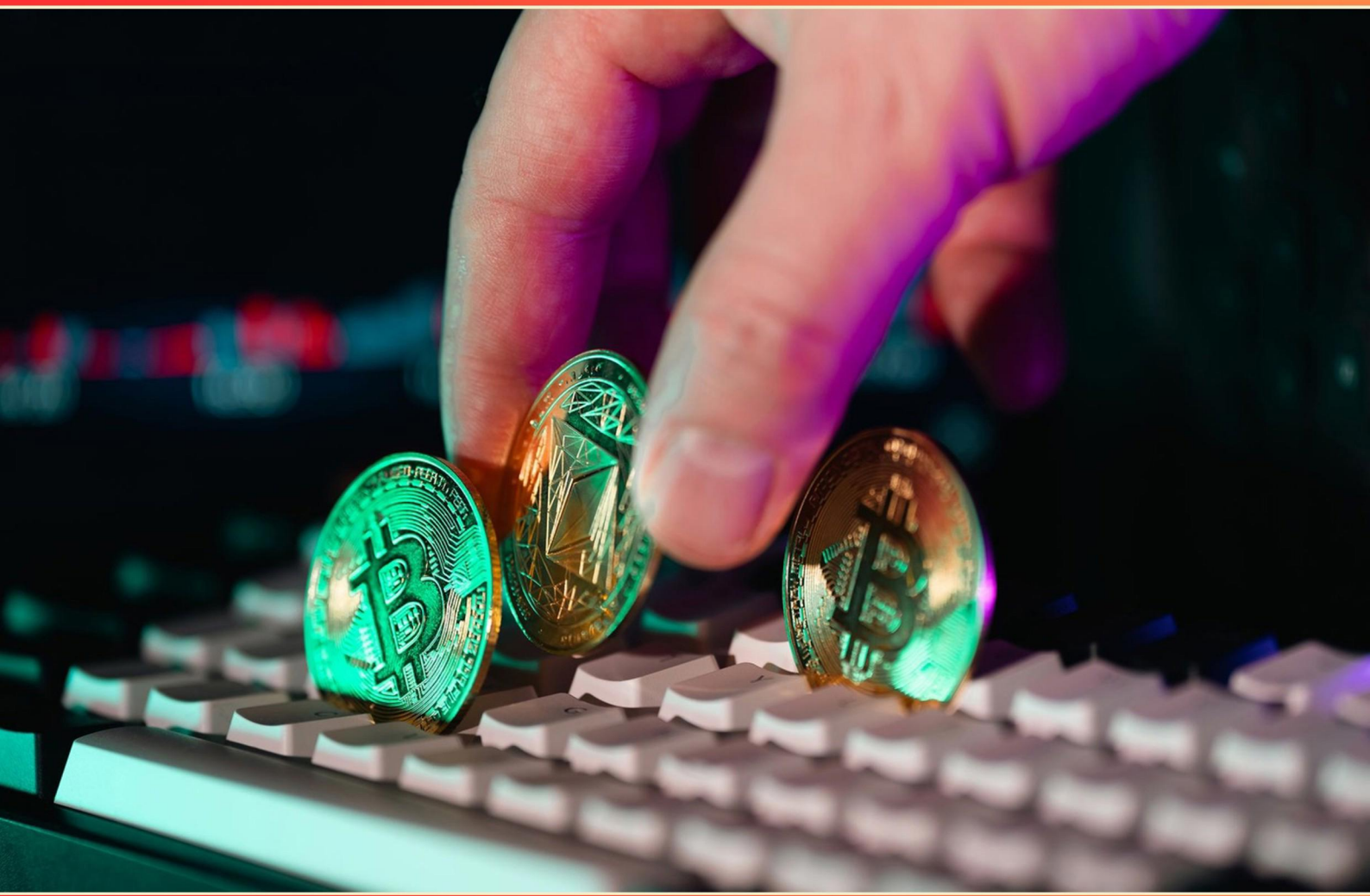
CERTIFIED THIRD-PARTY RISK PROFESSIONAL (CTPRP) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://ctprp.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. **What is third party risk management?**

   A. A process for identifying and managing the risks created when hiring a third party to provide goods and/or services

   B. A process for onboarding employees

   C. Auditing vendor pricing

   D. Managing internal software licenses

2. **Executive management level metrics focus on what and how many metrics typically?**

   A. Business and operational risks, about 60-80 metrics; changes are infrequent

   B. Financial accounting metrics, about 10 metrics; changes weekly

   C. Customer satisfaction metrics only, about 20 metrics; changes monthly

   D. Compliance-only metrics, about 5 metrics; changes quarterly

3. **What is the primary rationale for using a private cloud?**

   A. To keep a consistent level of security privacy, and governance control

   B. To minimize costs

   C. To maximize vendor lock-in

   D. To improve public accessibility

4. **Recovery Time Objective (RTO) is defined as which concept?**

   A. Point in time in the future at which you will be up and running again

   B. The time to restore backups from magnetic tapes

   C. The cost of DR site

   D. The number of data copies retained

5. **Primary Account Number (PAN) identifies the issuer and the cardholder account; this data is categorized as which?**

   A. Card Holder Data (CHD)/PCI data

   B. Personal Data

   C. Protected Health Information

   D. Electronic Health Records

6. A network security review should include which items?

A. Network device hardening standards; approval process when connecting new devices or firewall rule changes; outbound scans for malware, malicious/blacklisted sites, data policy violations

B. Password policy for users

C. Physical server cabling diagram

D. Marketing department budget

7. In Platform as a Service (PaaS), what is provided?

A. Hardware and software infrastructure for the development of business applications

B. User-facing software applications for sale

C. End-user devices

D. Customer support services

8. Which term describes entities that work on behalf of the organization but are not its employees?

A. Third party

B. Outsourcer

C. Fourth party/subcontractor

D. Vendor

9. What is the primary purpose of an information security policy?

A. Approved by mgmt and serves as foundation for the info security controls of an organization (includes incident mgmt and exception process)

B. To maximize marketing reach

C. To reduce payroll costs

D. To manage customer complaints

10. A risk assessment program should be approved by management and communicated to all appropriate constituents.

A. True

B. False

C. Not Sure

D. Not Applicable

Answers

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

Explanations

1. What is third party risk management?

A. A process for identifying and managing the risks created when hiring a third party to provide goods and/or services

B. A process for onboarding employees

C. Auditing vendor pricing

D. Managing internal software licenses

Third-party risk management is the process of identifying and managing the risks created when a third party provides goods or services. These risks come from vendors, suppliers, or service providers who may have access to your systems, networks, or data, or who perform critical business functions. The goal is to protect confidentiality, integrity, and availability of information, as well as regulatory compliance and business continuity. Effective third-party risk management involves several steps. Start with mapping who your external partners are and what data or access they handle. Then conduct due diligence to assess their security controls, privacy practices, and overall risk posture, often using evidence like security certifications, audits, or questionnaires. Develop a risk-based approach to contracts: include data protection addenda, clear security requirements, incident response and breach notification obligations, and rights to audit or assess changes. Implement mitigations where needed—controls, access restrictions, network segmentation, and monitoring. Finally, maintain ongoing vigilance through periodic reassessments, monitoring for changes in risk (like a vendor's security posture or regulatory status), and a plan for offboarding when a relationship ends to ensure data is returned or destroyed. In short, it focuses on the risks that come with engaging external parties and the controls you put in place to manage those risks throughout the relationship. The other activities—onboarding employees, auditing vendor pricing, or managing internal software licenses—address different areas such as internal HR processes, commercial due diligence, or internal asset management, and don't target the external risk landscape the way third-party risk management does.

2. Executive management level metrics focus on what and how many metrics typically?

A. Business and operational risks, about 60-80 metrics; changes are infrequent

B. Financial accounting metrics, about 10 metrics; changes weekly

C. Customer satisfaction metrics only, about 20 metrics; changes monthly

D. Compliance-only metrics, about 5 metrics; changes quarterly

Executive management metrics are meant to give a broad, strategic view by tracking business and operational risks across a wide set of indicators. A typical leadership dashboard uses roughly 60 to 80 metrics to cover the major risk areas, performance drivers, and outcomes without getting lost in granular detail. Keeping this metric set relatively stable and updating it infrequently helps leadership spot trends, compare performance over time, and make strategic decisions with confidence. In contrast, metrics focused only on financial accounting, customer satisfaction, or compliance tend to be narrower in scope and often change more frequently, which can dilute the big-picture perspective leaders need. This combination—a wide, risk- and performance-oriented view with infrequent changes—fits executive oversight best.

3. What is the primary rationale for using a private cloud?

A. To keep a consistent level of security privacy, and governance control

B. To minimize costs

C. To maximize vendor lock-in

D. To improve public accessibility

The main idea is that a private cloud is chosen to maintain consistent security, privacy, and governance across the cloud environment. Because resources are dedicated to a single organization, security configurations, compliance controls, data handling, and access policies can be standardized and enforced uniformly. This helps reduce the risk of gaps in protection and supports meeting regulatory and audit requirements. Costs and vendor dynamics are secondary considerations. Private clouds can entail higher ongoing costs due to dedicated resources and management, so minimizing costs isn't the primary rationale. While private clouds can influence vendor relationships, the goal isn't to maximize lock-in; the emphasis is on control and consistent governance. Public accessibility isn't the goal either, since a private cloud is about restricted, well-governed access rather than broad public exposure.

4. Recovery Time Objective (RTO) is defined as which concept?

A. Point in time in the future at which you will be up and running again

B. The time to restore backups from magnetic tapes

C. The cost of DR site

D. The number of data copies retained

RTO is the maximum downtime a business process can endure after a disruption and still avoid unacceptable impact. It's the target time by which systems, applications, or services must be restored and back online. This drives how quickly recovery efforts must proceed and what resources are needed to meet that deadline. For example, if the RTO is four hours, the recovery plan should ensure full operation within four hours of an outage. This concept is different from RPO, which is about how much data loss is acceptable, expressed in time. The choice that describes a point in the future by which you will be back up and running aligns with this idea, while the other choices refer to backup restoration timing, cost, or data copies, which are separate considerations.

5. Primary Account Number (PAN) identifies the issuer and the cardholder account; this data is categorized as which?

A. Card Holder Data (CHD)/PCI data

B. Personal Data

C. Protected Health Information

D. Electronic Health Records

PAN is categorized as Cardholder Data (CHD) under PCI DSS. Cardholder Data refers to the payment card details that identify the cardholder and the account, including the PAN along with the cardholder's name, expiration date, and service code. This classification exists to ensure PCI protections—strong controls for storage, processing, and transmission of card information such as encryption and access restrictions. It isn't healthcare data (Protected Health Information or Electronic Health Records) or simply Personal Data, which fall under different privacy frameworks. So, PAN falls squarely into Cardholder Data (CHD) within PCI data categories.

6. A network security review should include which items?

A. Network device hardening standards; approval process when connecting new devices or firewall rule changes; outbound scans for malware, malicious/blacklisted sites, data policy violations

B. Password policy for users

C. Physical server cabling diagram

D. Marketing department budget

A network security review focuses on how the network is configured, governed, and monitored to reduce risk. The best set of items includes network device hardening standards to minimize vulnerabilities, a formal approval process for connecting new devices or changing firewall rules to ensure changes are authorized and traceable, and outbound scans that check for malware, access to malicious or blacklisted sites, and data policy violations to detect threats and enforce policies. Together, these cover secure configuration, change governance, and outbound monitoring—the core activities of a network security review. While password policies are important for overall security, they belong to broader information security rather than the network-specific review. A physical cabling diagram is a physical layout artifact, not a security control, and a marketing budget is unrelated to network security.

7. In Platform as a Service (PaaS), what is provided?

A. Hardware and software infrastructure for the development of business applications

B. User-facing software applications for sale

C. End-user devices

D. Customer support services

PaaS delivers the platform layer that provides the hardware and software infrastructure developers use to build, test, and deploy business applications. It covers the runtime environment, development tools, databases, middleware, and hosting capabilities managed by the provider, so teams can focus on coding rather than managing servers, operating systems, or runtime components. The other options describe services outside this layer: user-facing applications for sale are typical of SaaS; end-user devices are hardware; and customer support services aren't what PaaS centers on.

8. Which term describes entities that work on behalf of the organization but are not its employees?

A. Third party

B. Outsourcer

C. Fourth party/subcontractor

D. Vendor

The idea being tested is identifying external entities that perform work for an organization but aren't employees. The broad term that covers all such entities is a third party. A third party can include vendors, contractors, consultants, and outsourcers—any external party engaged under a contract to help the organization achieve its goals. They are paid for their work and operate outside the organization's payroll, yet they carry out activities on the organization's behalf. In practice, this umbrella term matters for third-party risk management: you'd conduct due diligence, establish contract controls, specify security and compliance obligations, and maintain ongoing oversight of these relationships. The other terms describe more specific kinds of external relationships. An outsourcer focuses on taking over an entire function or process, which is a narrower definition. A vendor usually refers to a supplier of goods or standalone services, not necessarily someone who executes ongoing business work. A fourth party or subcontractor sits further down the chain, typically engaged by another provider rather than directly by the organization. So they describe parts of the relationship, but the broad, inclusive label that fits all such entities is third party.

9. What is the primary purpose of an information security policy?

A. Approved by mgmt and serves as foundation for the info security controls of an organization (includes incident mgmt and exception process)

B. To maximize marketing reach

C. To reduce payroll costs

D. To manage customer complaints

An information security policy provides governance and direction for how information assets must be protected. When senior management approves it, the policy carries authority across the organization and sets the scope, objectives, and expected behavior for everyone handling information. It serves as the foundation for all security controls by outlining the overarching rules that drive standards, procedures, incident response, and how exceptions are reviewed and approved. This ensures consistency in how security is implemented, enforced, and measured, and it supports auditability and regulatory compliance. The other goals mentioned—expanding marketing reach, reducing payroll costs, or managing customer complaints—do not address information security governance or the foundation for security controls.

10. A risk assessment program should be approved by management and communicated to all appropriate constituents.

A. True

B. False

C. Not Sure

D. Not Applicable

Approval by management and broad communication establish governance and accountability for risk assessment. When leadership formally approves the program, it gains legitimacy, aligns with strategic objectives, and secures the necessary resources and authority to operate consistently across the organization. Communicating the program to all appropriate constituents ensures people understand their roles, responsibilities, and the processes for identifying, evaluating, and mitigating risks, which is essential for effective execution. Without management approval, the program may lack funding or authority, and without wide communication, stakeholders may not follow the process or act on risk findings. So, this statement is true.

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://ctprp.examzify.com

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