# Certified Third-Party Risk Professional (CTPRP) Practice Exam (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. How should regulatory compliance be assessed for a vendor operating in multiple jurisdictions?**

**A. Map controls to applicable laws (e.g., GDPR/CCPA), review licenses/attestations, and assess cross-border transfer mechanisms.**

**B. Ignore jurisdictional differences and apply a single policy.**

**C. Only consider the laws of the vendor's home country.**

**D. Rely solely on contractual terms without regulatory consideration.**

**2. BC/DR testing primarily validates what aspect of business continuity plans?**

**A. Using actual written plans in exercises or tabletop reviews to test documentation**

**B. Performing routine software updates**

**C. Hiring new staff for crisis situations**

**D. Conducting financial risk assessments**

**3. Which framework is commonly used for mapping information security controls in third-party risk management?**

**A. ISO 27001**

**B. NIST Cybersecurity Framework (CSF)**

**C. COBIT**

**D. PCI DSS**

**4. Which artifact is listed among supporting due diligence artifacts as a detailed network component?**

**A. Sanitized network diagrams**

**B. Customer contracts**

**C. Employee handbooks**

**D. Security camera footage**

**5. Background verification includes which verification step?**

**A. Certification and license verification**

**B. Office supply ordering**

**C. Employee payroll processing**

**D. Travel approvals**

**6. Sensitive PII is PII used in conjunction with basic PII (for example, SSN card, Driver's License, DOB).**

- **A. PII used in conjunction with basic PII (i.e., SSN card, Driver's License, DOB)**
- **B. PII used alone**
- **C. PII that is publicly available**
- **D. PII that is not linked to an individual**

**7. Which of the following is explicitly listed as a data category for DLP scanning?**

- **A. SSN/National ID**
- **B. Credit card numbers**
- **C. Usernames**
- **D. Phone numbers**

**8. 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**

**9. Which statement best describes Software as a Service (SaaS)?**

- **A. Business application delivered over the Internet in which users interact with the application through a web browser.**
- **B. Infrastructure is managed and operated exclusively for one company.**
- **C. A combination of public and private cloud environments.**
- **D. An infrastructure shared by several organizations from a community.**

**10. Audits should ensure compliance with which category?**

- **A. Regulatory**
- **B. Marketing campaigns**
- **C. Product development**
- **D. Employee training**

# Answers

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

# Explanations

**1. How should regulatory compliance be assessed for a vendor operating in multiple jurisdictions?**

**A. Map controls to applicable laws (e.g., GDPR/CCPA), review licenses/attestations, and assess cross-border transfer mechanisms.**

**B. Ignore jurisdictional differences and apply a single policy.**

**C. Only consider the laws of the vendor's home country.**

**D. Rely solely on contractual terms without regulatory consideration.**

**Assessing regulatory compliance across multiple jurisdictions starts with understanding that each region can impose different requirements on how a vendor collects, processes, stores, and transfers data. The strong approach is to map the vendor's controls directly to the laws that apply in each place—for example, data protection rules like GDPR in Europe or CCPA in California—and then verify that the vendor has the appropriate licenses and attestations to demonstrate compliance. This also includes carefully examining how data moves across borders, ensuring that transfer mechanisms such as standard contractual clauses or other approved tools are in place and functioning, since cross-border data flows introduce additional legal obligations and risk. This approach matters because a one-size-fits-all policy can miss region-specific requirements, and focusing only on the vendor's home-country laws or relying solely on contractual terms without regulatory consideration can leave gaps that enforcement actions or data breaches could expose. By aligning controls to each applicable law, validating licenses and attestations, and confirming proper cross-border transfer mechanisms, you obtain a comprehensive view of regulatory risk across all jurisdictions where the vendor operates.**

**2. BC/DR testing primarily validates what aspect of business continuity plans?**

**A. Using actual written plans in exercises or tabletop reviews to test documentation**

**B. Performing routine software updates**

**C. Hiring new staff for crisis situations**

**D. Conducting financial risk assessments**

**BC/DR testing focuses on whether the documented procedures can be executed in a real scenario. By using the actual written plans in exercises or tabletop reviews, teams validate that the steps are clear, roles and responsibilities are understood, communication channels work, and recovery timelines are achievable. This process helps uncover gaps in the documentation—such as missing contacts, undefined decision triggers, or unclear sequence of actions—so the plan can function when needed. Other activities like routine software updates, hiring crisis staff, or conducting financial risk assessments are important but address separate aspects of operations, not the practical testing of the plan's documented procedures.**

## 3. Which framework is commonly used for mapping information security controls in third-party risk management?

**A. ISO 27001**

**B. NIST Cybersecurity Framework (CSF)**

**C. COBIT**

**D. PCI DSS**

**In third-party risk management, teams map security controls to vendor practices to understand risk exposure and identify gaps across the supply chain. The NIST Cybersecurity Framework (CSF) is commonly used for this because it provides a flexible structure with core functions (Identify, Protect, Detect, Respond, Recover) and a broad set of categories that align with many control baselines. Importantly, the CSF is designed to be cross-wwalkable to other standards and controls, such as NIST SP 800-53 and ISO 27001, which makes it easier to map a vendor's security controls to an organization's risk posture and to create a consistent, language-friendly view across multiple third parties. This adaptability and wide industry acceptance help organizations assess, compare, and improve security controls across a diverse vendor ecosystem. Other standards exist for specific purposes—ISO 27001 centers on implementing an information security management system, COBIT focuses on IT governance and control objectives, and PCI DSS targets payment card data protection. While these can inform third-party risk programs, they don't provide the same broad, cross-mwalkable framework for mapping and comparing controls across many different vendors as the NIST CSF.**

## 4. Which artifact is listed among supporting due diligence artifacts as a detailed network component?

**A. Sanitized network diagrams**

**B. Customer contracts**

**C. Employee handbooks**

**D. Security camera footage**

**Understanding what supports a thorough risk assessment in third-party due diligence involves recognizing artifacts that reveal how a network is actually laid out and protected. Sanitized network diagrams provide a detailed map of the network topology, showing components like firewalls, DMZs, routers, switches, VPN paths, and data flows, while removing sensitive details. This combination lets evaluators see where the attack surface lies, how segments are protected, and where controls are placed, which is exactly what you need to assess security posture without exposing secrets. The diagrams are kept sanitized so confidential information isn't disclosed, yet the essential structure remains visible for effective risk analysis. Other artifacts mentioned don't serve this specific purpose. A customer contract shows obligations and terms, not the technical architecture. An employee handbook covers internal policies rather than network design or security controls. Security camera footage doesn't illuminate how the network is built or protected.**

## 5. Background verification includes which verification step?

**A. Certification and license verification**

**B. Office supply ordering**

**C. Employee payroll processing**

**D. Travel approvals**

**Verifying professional certifications and licenses is a key part of background verification. This step confirms that the candidate truly holds the credentials they claim, that those credentials are valid and current, and that they were issued by the appropriate authority. It helps prevent resume fraud and ensures the person is legally qualified for roles that require regulated or specialized credentials. The other options don't fit background verification: ordering office supplies is a routine procurement task, payroll processing handles compensation data, and travel approvals are administrative workflow decisions.**

## 6. Sensitive PII is PII used in conjunction with basic PII (for example, SSN card, Driver's License, DOB).

**A. PII used in conjunction with basic PII (i.e., SSN card, Driver's License, DOB)**

**B. PII used alone**

**C. PII that is publicly available**

**D. PII that is not linked to an individual**

**Sensitive PII is data that becomes highly risky when it is combined with basic identifiers. Basic PII includes information that can identify a person by itself, such as name, address, or date of birth. When you add government-issued numbers like a Social Security Number or a driver's license number, or other highly identifying data, the set becomes sensitive because it greatly raises the potential for identity theft or fraud if disclosed. The example—SSN card, Driver's License, DOB—illustrates how those identifiers, when linked with other basic PII, escalate risk. Therefore, this description matches the idea that sensitive PII is PII used in conjunction with basic PII. PII used alone, publicly available PII, or PII not linked to an individual do not fit this concept.**

## 7. Which of the following is explicitly listed as a data category for DLP scanning?

**A. SSN/National ID**

**B. Credit card numbers**

**C. Usernames**

**D. Phone numbers**

**DLP scanning relies on predefined data categories to identify and protect sensitive information. SSN/National ID is explicitly listed as one of these categories because identifiers like a Social Security number or national ID are highly sensitive and tightly regulated. When a DLP system sees data that matches this category, it can apply strict controls, such as blocking transmission or triggering an alert, regardless of where the data appears (email, documents, or other channels). While other items like credit card numbers, usernames, and phone numbers can also be sensitive and monitored, the question highlights the category that is specifically named in many DLP taxonomies, which is SSN/National ID.**

## 8. 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.**

## 9. Which statement best describes Software as a Service (SaaS)?

**A. Business application delivered over the Internet in which users interact with the application through a web browser.**

**B. Infrastructure is managed and operated exclusively for one company.**

**C. A combination of public and private cloud environments.**

**D. An infrastructure shared by several organizations from a community.**

**The idea being tested is how software is delivered and accessed. In Software as a Service, the application is hosted by the provider in the cloud and you use it over the Internet, typically through a web browser. You don't install or manage the software on your own devices or servers; the vendor handles hosting, maintenance, security, and updates. This model enables quick deployment, scalable usage, and a subscription-based cost. The other options describe different cloud concepts. A private cloud describes infrastructure managed for a single organization, not software accessed over a browser. A hybrid cloud refers to a mix of public and private cloud environments. A community cloud describes infrastructure shared by multiple organizations with common concerns. These aren't SaaS.**

## 10. Audits should ensure compliance with which category?

**A. Regulatory**

**B. Marketing campaigns**

**C. Product development**

**D. Employee training**

**Audits are about verifying that an organization follows the laws, regulations, and external requirements that apply to its operations. The best fit is regulatory because audits are specifically designed to test compliance with those legal obligations and standards the organization must meet, including obligations related to third-party relationships, data protection, financial reporting, and security controls. This focus helps prevent penalties, fines, and reputational damage by showing the organization is exercising due care in staying within legal bounds. Marketing campaigns, product development, and employee training are important areas of business activity, but they are not the primary targets of audits for compliance. They can be reviewed for governance and process quality, but the core purpose of audits in this context is to confirm adherence to regulatory requirements.**

# 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!**