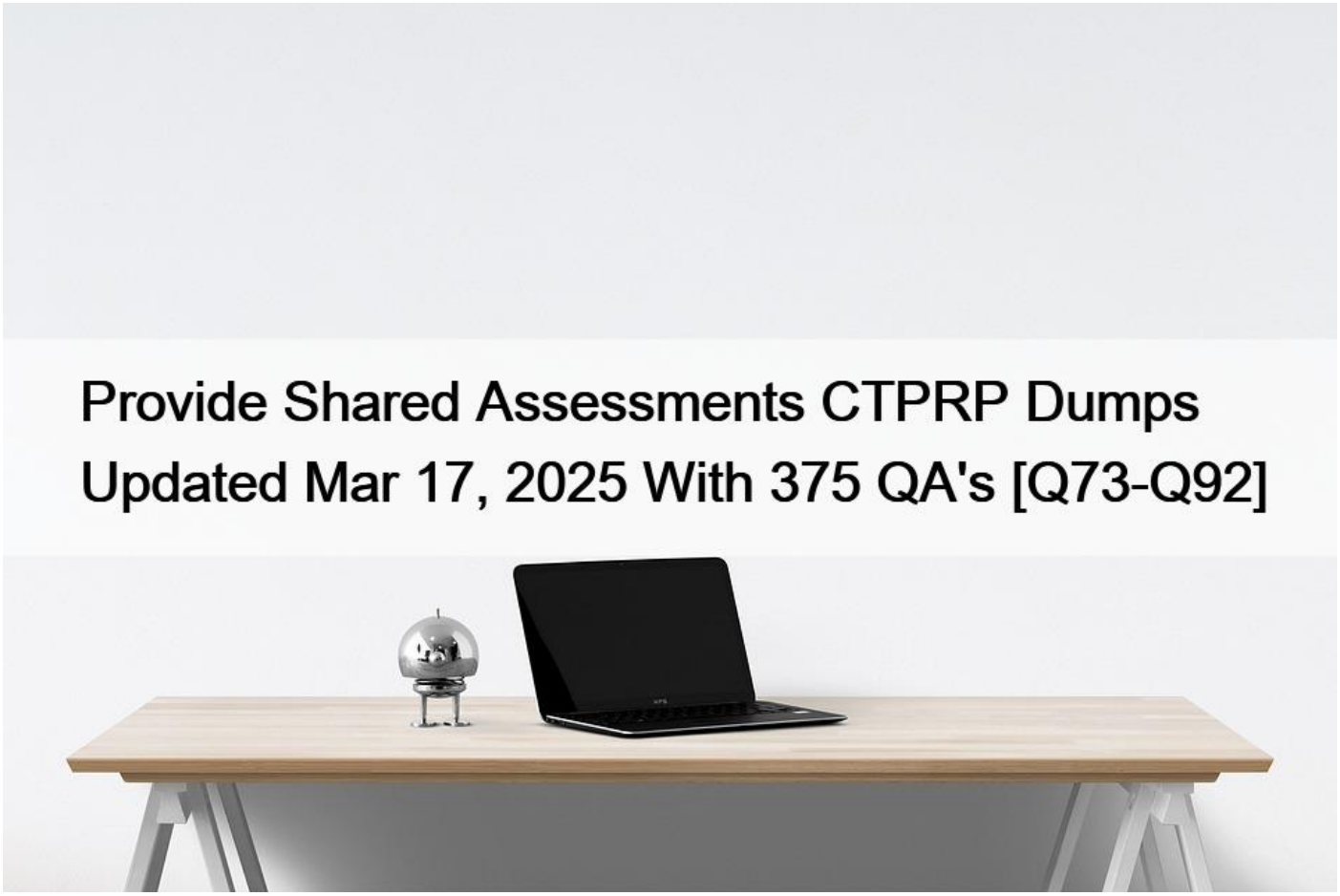
Provide Shared Assessments CTPRP Dumps Updated Mar 17, 2025 With 375 QA's [Q73-Q92



Provide Shared Assessments CTPRP Dumps Updated Mar 17, 2025 With 375 QA's Latest CTPRP Dumps for Success in Actual Shared Assessments Certified Q73. A healthcare company is evaluating a new cloud service for patient data management. What is essential for them to understand before finalizing their choice?

* The cost-effectiveness of the cloud solution
* The physical location of the cloud servers
* The type of cloud model and security roles involved
* Level of customer support provided by the cloud service

For a healthcare company managing sensitive patient data, understanding the type of cloud model and the specific security roles involved is fundamental to ensure that the chosen cloud service adequately meets security and compliance requirements.

Q74. In the context of third-party risk management, what tool is used to gather information about a vendor’s operations and compliance?

* Annual financial statements review
* Detailed risk analysis report
* Self-assessment questionnaire
* Customer satisfaction survey results

The self-assessment questionnaire is a key tool in third-party risk management, designed to collect detailed information on the

vendor’s operations, controls, and compliance status, helping organizations make informed decisions with minimal resources.

Q75. A company’s emergency response plan fails to adequately address flood scenarios, despite being located in a flood-prone are a. What is the most critical update needed in their emergency preparedness plan?
* Adding general guidelines for all types of natural disasters
* Updating the contact information for emergency services
* Incorporating specific procedures and resources to handle potential flooding
* Increasing the stock of emergency supplies like food and water

In areas prone to flooding, it is critical to have specific procedures and resources in place to address flood scenarios effectively. This includes plans for safeguarding equipment, ensuring the safety of personnel, and managing continuity of operations during and after a flood.

Q76. A risk register typically includes the risk’s _____, impact, and likelihood.
* Timing
* Cost
* Description
* Source

Including the risk description is crucial as it provides clear and essential details about the nature of the risk, which aids in understanding and managing the risk properly.

Q77. Considering multi-factor authentication, which example represents a correct implementation for accessing a corporate network?
* Using a password, a received SMS code, and a biometric scan
* Using a password and answering a personal security question
* Using a biometric scan and a device the user has, like a smart card
* Using a security token and a mobile app notification approval

Using a password, receiving an SMS code, and undergoing a biometric scan embodies the principle of multi-factor authentication by combining something the user knows, has, and is, thus providing a robust defense against unauthorized access.

Q78. Scenario: An organization uses an application with extensive remote connectivity options. During a security review, what aspect should be the focal point to understand the potential risks?
* Examine the processing speed of the application to ensure efficiency
* Evaluate the licensing terms and conditions for any security implications
* Review the customer support effectiveness for managing remote access issues
* Assess the remote connectivity options to identify potential vulnerabilities

The correct answer highlights that remote connectivity options are vital to understand potential vulnerabilities, as they can expose the application to unauthorized access or attacks if not properly secured.

Q79. What is the primary purpose of analyzing responses from a vendor questionnaire?
* To identify any gaps, issues, or risks that may pose a threat to the organization or its customers
* To assess the vendor’s alignment with the organization’s strategic objectives
* To compare the vendor’s performance against industry benchmarks
* To finalize the contract terms and conditions with the vendor

The primary purpose of analyzing responses from a vendor questionnaire is to identify any potential gaps, issues, or risks that could threaten the organization or its customers. This analysis helps in understanding vulnerabilities and areas needing attention to ensure vendor alignment with the organization’s safety and compliance standards.

Q80. Remote wipe is typically utilized to ensure no company data remains on a _____.
* device before it is issued to a new employee

* device when changing departments within a company
* device after completing a company project
* device after it is lost or stolen

Remote wipe ensures that no residual data remains on a device after it is lost or stolen, which is critical for protecting company information and reducing the risk of data breaches.

Q81. Which activity reflects the concept of vendor management?
* Managing service level agreements
* Scanning and collecting information from third party web sites
* Reviewing and analyzing external audit reports
* Receiving and analyzing a vendor’s response to & questionnaire

Vendor management is the process of coordinating with vendors to ensure excellent service to your customers12. It involves activities such as selecting vendors, negotiating contracts, controlling costs, reducing vendor-related risks and ensuring service delivery12. One of the key activities of vendor management is managing service level agreements (SLAs), which are contracts that define the expectations and obligations of both parties regarding the quality, quantity, and timeliness of the goods or services provided3. SLAs help to monitor and measure vendor performance, identify and resolve issues, and enforce penalties or rewards based on the agreed-upon metrics3. The other options are not correct because they do not reflect the concept of vendor management as a whole, but rather specific aspects or tools of vendor management. Scanning and collecting information from third party web sites, reviewing and analyzing external audit reports, and receiving and analyzing a vendor’s response to a questionnaire are all examples of methods or sources of information that can be used to conduct vendor due diligence, risk assessment, or performance evaluation, but they are not the only or the most important activities of vendor management. References:

* What is Vendor Management? Definition, Process, and Tools

* What is vendor management? | Definition & Process | Taulia

* Essential Guide to Vendor Management | Smartsheet, section “Service Level Agreements”

Q82. Describe a scenario where a vendor’s inadequate patch management leads to a data breach.
* Regular security audits miss critical vulnerabilities due to a lack of comprehensive coverage.
* A vendor fails to apply a critical security update, allowing hackers to exploit a known vulnerability and access sensitive data.
* A security patch conflicts with existing software, causing system instability and data loss.
* An outdated firewall allows malware to infiltrate the network, unnoticed during routine checks.

In the scenario where a vendor fails to apply a critical update, it directly leads to a security breach when hackers exploit the vulnerability. This highlights the importance of timely patch management to secure network systems against known risks.

Q83. Which of the following BEST reflects the risk of a ‘shadow IT” function?
* “Shadow IT” functions often fail to detect unauthorized use of information assets
* “Shadow IT” functions often lack governance and security oversight
* inability to prevent “shadow IT’ functions from using unauthorized software solutions
* Failure to implement strong security controls because IT is executed remotely

Shadow IT refers to the use of IT systems, services, or devices that are not authorized, approved, or supported by the official IT department. Shadow IT can pose significant risks to an organization’s data security, compliance, performance, and reputation. One of the main risks of shadow IT is that it often lacks governance and security oversight. This means that the shadow IT functions may not follow the established policies, standards, and best practices for IT management, such as data protection, access control, encryption, backup, patching, auditing, and reporting. This can expose the organization to various threats, such as data breaches, cyberattacks, malware infections, legal liabilities, regulatory fines, and reputational damage. Additionally, shadow IT can create operational inefficiencies, compatibility issues, duplication of efforts, and increased costs for the organization.

According to the web search results from the search_web tool, shadow IT is a common and growing phenomenon in many

organizations, especially with the proliferation of cloud-based services and applications. Some of the articles suggest the following best practices for managing and mitigating shadow IT risks123:

* Performing SaaS assessments to proactively detect shadow IT

* Prioritizing user experience (UX) and providing support for integrating tools

* Streamlining user account and identity management

* Using operating systems and devices with which employees are comfortable

* Compromising and collaborating with users to minimize shadow IT risks

* Educating and training users on the security risks and consequences of shadow IT

* Establishing clear policies and guidelines for IT procurement and usage

* Creating a culture of trust and transparency between IT and business units Therefore, the verified answer to the question is B. “Shadow IT” functions often lack governance and security oversight.

References:

* Shadow IT Explained: Risks & Opportunities – BMC Software

* Start reducing your organization’s Shadow IT risk in 3 steps

* What is shadow IT? – Article | SailPoint

Q84. Which factor is least critical in determining the application’s security or functionality?
* The aesthetic design of the user interface
* The size of the application in terms of disk space
* The complexity of the application’s backend infrastructure
* The number of software releases
The correct answer indicates that the number of software releases does not directly impact the application’s security or functionality. While it may reflect the maturity of the development process, it is not as critical as other factors.

Q85. Which entity traditionally forms the third line of defense in an organization’s risk management structure?
* The risk management office
* The internal audit function
* The executive management team
* The compliance department
The internal audit function is designated as the third line of defense, providing an independent and unbiased review to ensure that risk controls and governance frameworks are effective, separate from direct business activities.

Q86. Which of the following statements BEST represent the relationship between incident response and incident notification plans?
* Cybersecurity incident response programs have the same scope and objectives as privacy incident notification procedures
* All privacy and security incidents should be treated alike until analysis is performed to quantify the number of records impacted
* Security incident response management is only included in crisis communication for externally reported events
* A security incident may become a security breach based upon analysis and trigger the organization’s incident notification or crisis communication process

Incident response and incident notification are two related but distinct processes that organizations should follow when dealing with security incidents. Incident response is the process of identifying, containing, analyzing, eradicating, and recovering from security incidents, while incident notification is the process of communicating the relevant information about the incident to the appropriate internal and external stakeholders, such as senior management, regulators, customers, and media12.

Not all security incidents are security breaches, which are defined as unauthorized access to or disclosure of sensitive or confidential information that could result in harm to the organization or individuals3. A security incident may become a security breach based on the analysis of the impact, scope, and severity of the incident, as well as the applicable legal and regulatory requirements. When a security breach is confirmed or suspected, the organization should trigger its incident notification or crisis communication process, which should include the following elements:

* A clear definition of roles and responsibilities for notification and communication

* A list of internal and external stakeholders who need to be notified and their contact information

* A set of predefined templates and messages for different types of incidents and audiences

* A communication strategy and timeline that aligns with the incident response plan and the business continuity plan

* A feedback mechanism to monitor and measure the effectiveness of the communication and adjust as needed Incident notification and communication are critical for managing the reputation, trust, and compliance of the organization, as well as for mitigating the potential legal, financial, and operational consequences of a security breach. References:

* 1: Incident Response Plan: Frameworks and Steps

* 2: A Guide to Incident Response Plans, Playbooks, and Policy

* 3: What is Incident Response? Plan and Steps

* : Incident Response and Breach Notification

* : Incident Response Communication: Best Practices

* : The Importance of Incident Response Communication

Q87. What type of documentation is crucial for verifying a CSP’s commitment to maintaining security standards?
* Annual financial statements and operational budgets.
* Monthly performance reviews and user access logs.
* Service level agreements, security certifications, and audit attestation reports.
* Weekly incident reports and data breach notifications.
Service level agreements, security certifications, and audit attestation reports are critical as they collectively demonstrate the CSP’s adherence to agreed standards and regulations, providing a comprehensive view of the CSP’s commitment to security.

Q88. Given the security measures listed, which one would not directly impact the evaluation of remote access risks?
* Implementing end-to-end encryption for data in transit to safeguard against interception.
* Employing multifactor authentication to verify the identity of users accessing systems remotely.
* Application whitelisting, as it focuses on limiting software execution based on pre-established security policies.
* Remote desktop protocol (RDP) security, as it directly relates to the safety of remote desktop connections.
Application whitelisting’s focus is specifically on controlling application execution based on a list of approved software,

which does not directly deal with the integrity of remote access connections or the authentication and authorization processes involved in remote access scenarios.

Q89. A company discovers that an employee is using a company-issued device for personal business. According to typical end-user device policies, which of the following actions is most justified?
* The IT department should isolate the device to prevent any organizational data from being compromised.
* The employee may face reprimands or restrictions according to the severity of the misuse.
* An investigation is launched to determine if any personal data was collected from the device.
* The employee’s device is immediately confiscated and they are suspended from work.

Typical end-user device policies outline acceptable use, and using company devices for personal business often violates these stipulations, thus justifying disciplinary actions depending on the specifics of the policy.

Q90. Why is continuous monitoring of network activity important when a third party has access to an organization’s network?
* It helps in reducing the operational costs associated with network management.
* It ensures all vendor activities are fully automated and require minimal oversight.
* It facilitates better collaboration between the organization and the vendor.
* It allows for the detection and mitigation of security threats in real time.

Continuous monitoring of network activity is important because it enables the organization to detect unusual or unauthorized activities early, allowing for timely interventions to prevent or mitigate potential security incidents.

Q91. What does an unrecoverable data loss after a system restore indicate about the Recovery Point Objective (RPO)?
* It shows that the incident response was not initiated in a timely manner.
* It reflects an adequate level of preparedness and compliance with industry standards.
* It suggests the Recovery Time Objective (RTO) metrics were not calculated correctly.
* It indicates that the Recovery Point Objective was not met as the data loss exceeded the allowable period.

The Recovery Point Objective (RPO) defines the maximum period during which data can be lost due to an incident. If data restoration after a system failure results in unrecoverable data loss exceeding this period, it signifies that the RPO was not achieved, hence the disaster recovery strategies need reassessment to align with the established RPO.

Q92. When working with third parties, which of the following requirements does not reflect a “Zero Trust” approach to access management?
* Utilizing a solution that allows direct access by third parties to the organization’s network
* Ensure that access is granted on a per session basis regardless of network location, user, or device
* Implement device monitoring, continual inspection and monitoring of logs/traffic
* Require that all communication is secured regardless of network location

A Zero Trust approach to access management is based on the principle of verifying every access request as if it originates from an open network, regardless of the source, destination, or context. This means that no implicit trust is granted based on network location, user identity, or device status. Instead, every access request is evaluated based on multiple factors, such as user credentials, device health, data sensitivity, and threat intelligence. A Zero Trust approach also requires that all communication is encrypted and protected, and that access is granted on a per session basis with the least privilege principle123.

Utilizing a solution that allows direct access by third parties to the organization’s network does not reflect a Zero Trust approach, because it implies that the network perimeter is a reliable boundary for security and trust.

This assumption is risky, because it exposes the organization to potential breaches and attacks from compromised or malicious third parties, who may have access to sensitive data and resources without proper verification or protection. A Zero Trust approach would require that third parties use secure and isolated channels to access the organization’s network, such as VPNs, proxies, or gateways, and that their access is monitored and controlled based on granular policies and conditions123. References:

* Zero Trust part 1: Identity and access management

* Zero Trust Model – Modern Security Architecture | Microsoft Security

* Zero Trust identity and access management development best practices …

Changing the Concept of CTPRP Exam Preparation 2025:
https://www.testkingfree.com/Shared-Assessments/CTPRP-practice-exam-dumps.html]