KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **CTPRP**

Title : Certified Third-Party Risk Professional (CTPRP)

Version : DEMO

1.Which of the following actions is an early step when triggering an Information Security Incident Response Program?
A. Implementing processes for emergency change control approvals
B. Requiring periodic changes to the vendor's contract for breach notification
C. Assessing the vendor's Business Impact Analysis (BIA) for resuming operations
D. Initiating an investigation of the unauthorized disclosure of data
Answer: D
Explanation:
According to the NIST Computer Security Incident Handling Guide1, one of the first steps in responding to an incident is to identify the scope, nature, and source of the incident. This involves gathering evidence, analyzing logs, interviewing witnesses, and performing forensic analysis. The goal is to determine the extent of the compromise, the type of attack, the identity or location of the attacker, and the potential impact on the organization and its stakeholders. This step is essential for containing the incident, mitigating the damage, and preventing further escalation or recurrence.
Reference: NIST Computer Security Incident Handling Guide1, Section 3.2.2 Identification
Cisco What Is an Incident Response Plan for IT?2, Section 2. Respond
CrowdStrike Incident Response [Beginner’s Guide]3, Section 3. Incident Response Steps

2.When evaluating compliance artifacts for change management, a robust process should include the following attributes:
A. Approval, validation, auditable.
B. Logging, approvals, validation, back-out and exception procedures
C. Logging, approval, back-out.
D. Communications, approval, auditable.
Answer: B
Explanation:
Change management is the process of controlling and documenting any changes to the scope, objectives, requirements, deliverables, or resources of a project or a program. Change management ensures that the impact of any change is assessed and communicated to all stakeholders, and that the changes are implemented in a controlled and coordinated manner. Compliance artifacts are the documents, records, or reports that demonstrate the adherence to the change management process and the regulatory or industry standards.
A robust change management process should include the following attributes:
Logging: This means that any change request or proposal is recorded in a change log or a change register, along with the details of the change initiator, the change description, the change category, the change priority, the change status, and the change history. Logging helps to track and monitor the progress and outcome of each change, and to provide an audit trail for compliance purposes.
Approvals: This means that any change request or proposal is reviewed and approved by the appropriate authority or stakeholder, such as the project manager, the sponsor, the customer, the steering committee, or the regulatory body. Approvals help to ensure that the change is justified, feasible, aligned with the project or program objectives, and acceptable to the affected parties.
Validation: This means that any change request or proposal is verified and tested to ensure that it meets the quality standards, the functional and non-functional requirements, and the expected benefits and outcomes. Validation helps to ensure that the change is implemented correctly, effectively, and efficiently,

and that it does not introduce any errors, defects, or risks.
Back-out and exception procedures: This means that any change request or proposal has a contingency plan or a rollback plan in case the change fails, causes problems, or is rejected. Back-out and exception procedures help to minimize the negative impact of the change, and to restore the original state or the baseline of the project or program. They also help to handle any deviations or issues that may arise during the change implementation or the change review.
Reference: CTPRP Job Guide
An Agile Approach to Change Management
CM Overview
Management Artifacts and its Types
Achieving Regulatory and Industry Standards Compliance with the Scaled Agile Framework
8 Steps for an Effective Change Management Process

3.Which factor describes the concept of criticality of a service provider relationship when determining vendor classification?
A. Criticality is limited to only the set of vendors involved in providing disaster recovery services
B. Criticality is determined as all high risk vendors with access to personal information
C. Criticality is assigned to the subset of vendor relationships that pose the greatest impact due to their unavailability
D. Criticality is described as the set of vendors with remote access or network connectivity to company systems
Answer: C
Explanation:
Criticality is a measure of how essential a service provider is to the organization’s core business functions and objectives. It reflects the potential consequences of a service disruption or failure on the organization’s operations, reputation, compliance, and financial performance. Criticality is not the same as risk, which is the likelihood and severity of a negative event occurring. Criticality helps to prioritize the risk assessment and mitigation efforts for different service providers based on their relative importance to the organization. Criticality is not limited to a specific type of service, such as disaster recovery or personal information, nor is it determined by the mode of access or connectivity. Criticality is assigned to the service providers that have the greatest impact on the organization’s ability to deliver its products or services to its customers and stakeholders in a timely and satisfactory manner.
Reference: Shared Assessments. (2020). Certified Third Party Risk Professional (CTPRP) Study Guide1
Milliman. (2017). Defining “critical or important functions or activities” for outsourcing purposes2
Webster, C. and Sundaram, D.S. (2009). Effect of service provider’s communication style on customer satisfaction in professional services setting: the moderating role of criticality and service nature. Journal of Services Marketing, 23(2), 103-1131

4.Which of the following statements is FALSE about Data Loss Prevention Programs?
A. DLP programs include the policy, tool configuration requirements, and processes for the identification, blocking or monitoring of data
B. DLP programs define the consequences for non-compliance to policies
C. DLP programs define the required policies based on default tool configuration
D. DLP programs include acknowledgement the company can apply controls to remove any data

Answer: C
Explanation:
Data Loss Prevention (DLP) programs are not based on default tool configuration, but on the specific needs and risks of the organization. DLP programs should be tailored to the data types, locations, flows, and users that are relevant to the business. DLP programs should also align with the regulatory and contractual obligations, as well as the data risk appetite, of the organization. Default tool configuration may not adequately address these factors and may result in either over-blocking or under-protecting data. Therefore, statement C is false about DLP programs.
Reference:
1: The Best Data Loss Prevention Software Tools - Comparitech
2: Build a Successful Data Loss Prevention Program in 5 Steps - Gartner
3: What is data loss prevention (DLP)? | Microsoft Security

5.Which of the following is typically NOT included within the scape of an organization's network access policy?
A. Firewall settings
B. Unauthorized device detection
C. Website privacy consent banners
D. Remote access
Answer: C
Explanation:
A network access policy is a set of rules and conditions that define how authorized users and devices can access the network resources and services of an organization. It typically includes the following elements12:
Firewall settings: These are the rules that control the incoming and outgoing network traffic based on the source, destination, protocol, and port of the packets. Firewall settings help to protect the network from unauthorized or malicious access, and to enforce the network security policy of the organization.
Unauthorized device detection: This is the process of identifying and preventing unauthorized devices from accessing the network. Unauthorized devices can pose a security risk to the network, as they may not comply with the security standards and policies of the organization, or they may be compromised by malware or hackers. Unauthorized device detection can be done by using various methods, such as network access control (NAC), network admission control (NAC), or 802.1X authentication.
Remote access: This is the ability of authorized users to access the network resources and services of the organization from a remote location, such as a home office, a hotel, or a public hotspot. Remote access can be provided by using various technologies, such as virtual private networks (VPNs), remote desktop services (RDS), or remote access services (RAS). Remote access requires a secure and reliable connection, and it must comply with the network access policy of the organization.
Website privacy consent banners: These are the messages that appear on websites to inform the visitors about the use of cookies and other tracking technologies, and to obtain their consent for such use. Website privacy consent banners are part of the website privacy policy, which is a legal document that discloses how the website collects, uses, and protects the personal data of the visitors. Website privacy consent banners are not related to the network access policy of the organization, as they do not affect how the users and devices can access the network resources and services of the organization.
Therefore, the correct answer is C. Website privacy consent banners, as they are typically not included

within the scope of an organization’s network access policy.
Reference:
1: Network Policy Server (NPS) | Microsoft Learn
2: Network Access Policy | University Policies