Shared-Assessments

Exam Questions CTPRP

Certified Third-Party Risk Professional (CTPRP)

NEW QUESTION 1
Which type of contract provision is MOST important in managing Fourth-Nth party risk after contract signing and on-boarding due diligence is complete?

A. Subcontractor notice and approval
B. Indemnification and liability
C. Breach notification
D. Right to audit

Answer: A

NEW QUESTION 2
Which example of analyzing a vendor's response should trigger further investigation of their information security policies?

A. Determination that the security policies include contract or temporary workers
B. Determination that the security policies do not specify any requirements for third party governance and oversight
C. Determination that the security policies are approved by management and available to constituents including employees and contract workers
D. Determination that the security policies are communicated to constituents including full and part-time employees

Answer: B

NEW QUESTION 3
Which statement provides the BEST description of inherent risk?

A. inherent risk is the amount of risk an organization can incur when there is an absence of controls
B. Inherent risk is the level of risk triggered by outsourcing & product or service
C. Inherent risk is the amount of risk an organization can accept based on their risk tolerance
D. Inherent risk is the level of risk that exists with all of the necessary controls in place

Answer: A

NEW QUESTION 4
Which of the following would be a component of an arganization??s Ethics and Code of Conduct Program?

A. Participation in the company's annual privacy awareness program
B. A disciplinary process for non-compliance with key policies, including formal termination or change of status process based on non-compliance
C. Signing acknowledgement of Acceptable Use policy for use of company assets
D. A process to conduct periodic access reviews of critical Human Resource files

Answer: B

NEW QUESTION 5
Which factor in patch management is MOST important when conducting postcybersecurity incident analysis related to systems and applications?

A. Configuration
B. Log retention
C. Approvals
D. Testing

Answer: D

NEW QUESTION 6
Which set of procedures is typically NOT addressed within data privacy policies?

A. Procedures to limit access and disclosure of personal information to third parties
B. Procedures for handling data access requests from individuals
C. Procedures for configuration settings in identity access management
D. Procedures for incident reporting and notification

Answer: C

NEW QUESTION 7
Data loss prevention in endpoint security is the strategy for:

A. Assuring there are adequate data backups in the event of a disaster
B. Preventing exfiltration of confidential information by users who access company systems
C. Enabling high-availability to prevent data transactions from loss
D. Preventing malware from entering secure systems used for processing confidential information

Answer: B

NEW QUESTION 8
Which statement BEST represents the primary objective of a third party risk assessment:

A. To assess the appropriateness of non-disclosure agreements regarding the organization's systems/data
B. To validate that the vendor/service provider has adequate controls in place based on the organization's risk posture
C. To determine the scope of the business relationship
D. To evaluate the risk posture of all vendors/service providers in the vendor inventory

Answer: B

NEW QUESTION 9
Which of the following changes to the production environment is typically NOT subject to the change control process?

A. Change in network
B. Change in systems
C. Change to administrator access
D. Update to application

Answer: C

NEW QUESTION 10
Which of the following indicators is LEAST likely to trigger a reassessment of an existing vendor?

A. Change in vendor location or use of new fourth parties
B. Change in scope of existing work (e.g., new data or system access)
C. Change in regulation that impacts service provider requirements
D. Change at outsourcer due to M&A

Answer: D

NEW QUESTION 10
Which statement is FALSE regarding the primary factors in determining vendor risk classification?

A. The geographic area where the vendor is located may trigger specific regulatory obligations
B. The importance to the outsourcer's recovery objectives may trigger a higher risk tier
C. The type and volume of personal data processed may trigger a higher risk rating based on the criticality of the systems
D. Network connectivity or remote access may trigger a higher vendor risk classification only for third parties that process personal information

Answer: D

NEW QUESTION 13
If a system requires ALL of the following for accessing its data: (1) a password, (2) a security token, and (3) a user's fingerprint, the system employs:

A. Biometric authentication
B. Challenge/Response authentication
C. One-Time Password (OTP) authentication
D. Multi-factor authentication

Answer: D

NEW QUESTION 16
Which statement is NOT a method of securing web applications?

A. Ensure appropriate logging and review of access and events
B. Conduct periodic penetration tests
C. Adhere to web content accessibility guidelines
D. Include validation checks in SDLC for cross site scripting and SOL injections

Answer: C

NEW QUESTION 21
An organization has experienced an unrecoverable data loss event after restoring a system. This is an example of:

A. A failure to conduct a Root Cause Analysis (RCA)
B. A failure to meet the Recovery Time Objective (RTO)
C. A failure to meet the Recovery Consistency Objective (RCO)
D. A failure to meet the Recovery Point Objective (RPO)

Answer: D

NEW QUESTION 23
Which of the following statements is FALSE regarding a virtual assessment:

A. Virtual assessment agendas and planning should identify who should be available for interviews
B. Virtual assessment planning should identify what documentation is available for review prior to and during the assessment
C. Virtual assessments should be used to validate or confirm understanding of key controls, and not be used simply to review questionnaire responses
D. Virtual assessments include using interviews with subject matter experts since controls evaluation and testing cannot be performed virtually

Answer: D

NEW QUESTION 25
For services with system-to-system access, which change management requirement MOST effectively reduces the risk of business disruption to the outsourcer?

A. Approval of the change by the information security department
B. Documenting sufficient time for quality assurance testing
C. Communicating the change to customers prior ta deployment to enable external acceptance testing
D. Documenting and legging change approvals

Answer: B

NEW QUESTION 27
Which cloud deployment model is primarily used for load balancing?

A. Public Cloud
B. Community Cloud
C. Hybrid Cloud
D. Private Cloud

Answer: C

NEW QUESTION 32
Your organization has recently acquired a set of new global third party relationships due to M&A. You must define your risk assessment process based on your due diligence standards. Which risk factor is LEAST important in defining your requirements?

A. The risk of increased expense to conduct vendor assessments based on client contractual requirements
B. The risk of natural disasters and physical security risk based on geolocation
C. The risk of increased government regulation and decreased political stability based on country risk
D. The financial risk due to local economic factors and country infrastructure

Answer: A

NEW QUESTION 33
Which action statement BEST describes an assessor calculating residual risk?

A. The assessor adjusts the vendor risk rating prior to reporting the findings to the business unit
B. The assessor adjusts the vendor risk rating based on changes to the risk level after analyzing the findings and mitigating controls
C. The business unit closes out the finding prior to the assessor submitting the final report
D. The assessor recommends implementing continuous monitoring for the next 18 months

Answer: B

NEW QUESTION 35
The set of shared values and beliefs that govern a company??s attitude toward risk is known as:

A. Risk tolerance
B. Risk treatment
C. Risk culture
D. Risk appetite

Answer: C

NEW QUESTION 37
When updating TPRM vendor classification requirements with a focus on availability, which risk rating factors provide the greatest impact to the analysis?

A. Type of data by classification; volume of records included in data processing
B. Financial viability of the vendor; ability to meet performance metrics
C. Network connectivity; remote access to applications
D. impact on operations and end users; impact on revenue; impact on regulatory compliance

Answer: D

NEW QUESTION 39
When measuring the operational performance of implementing a TPRM program, which example is MOST likely to provide meaningful metrics?

A. logging the number of exceptions to existing due diligence standards
B. Measuring the time spent by resources for task and corrective action plan completion
C. Calculating the average time to remediate identified corrective actions
D. Tracking the number of outstanding findings

Answer: C

NEW QUESTION 42

Which of the following topics is LEAST important when evaluating a service provider's Security and Privacy Awareness Program?

A. Training on phishing and social engineering risks and expected actions for employees and contractors
B. Training on whistleblower compliance issue reporting mechanisms
C. Training that is designed based on role, job scope, or level of access
D. Training on acceptable use and data safeguards based on organization's policies

Answer: B

NEW QUESTION 43
Which factor is less important when reviewing application risk for application service providers?

A. Remote connectivity
B. The number of software releases
C. The functionality and type of data the application processes
D. API integration

Answer: B

NEW QUESTION 47
Which factor is MOST important when scoping assessments of cloud-based third parties that access, process, and retain personal data?

A. The geographic location of the vendor's outsourced datacenters since assessments are only required for international data transfers
B. The identification of the type of cloud hosting deployment or service model in order to confirm responsibilities between the third party and the cloud hosting provider
C. The definition of requirements for backup capabilities for power generation and redundancy in the resilience plan
D. The contract terms for the configuration of the environment which may prevent conducting the assessment

Answer: B

NEW QUESTION 50
Which of the following data safeguarding techniques provides the STRONGEST assurance that data does not identify an individual?

A. Data masking
B. Data encryption
C. Data anonymization
D. Data compression

Answer: C

NEW QUESTION 55
Which statement is FALSE when describing the differences between security vulnerabilities and security defects?

A. A security defect is a security flaw identified in an application due to poor coding practices
B. Security defects should be treated as exploitable vulnerabilities
C. Security vulnerabilities and security defects are synonymous
D. A security defect can become a security vulnerability if undetected after migration into production

Answer: C

NEW QUESTION 57
A contract clause that enables each party to share the amount of information security risk is known as:

A. Limitation of liability
B. Cyber Insurance
C. Force majeure
D. Mutual indemnification

Answer: D

NEW QUESTION 60
Which of the following factors is LEAST likely to trigger notification obligations in incident response?

A. Regulatory requirements
B. Data classification or sensitivity
C. Encryption of data
D. Contractual terms

Answer: C

NEW QUESTION 64
Which statement BEST reflects the factors that help you determine the frequency of cyclical assessments?

A. Vendor assessments should be conducted during onboarding and then be replaced by continuous monitoring
B. Vendor assessment frequency should be based on the level of risk and criticality of the vendor to your operations as determined by their vendor risk score

C. Vendor assessments should be scheduled based on the type of services/products provided
D. Vendor assessment frequency may need to be changed if the vendor has disclosed a data breach

Answer: B

NEW QUESTION 68
An IT asset management program should include all of the following components EXCEPT:

A. Maintaining inventories of systems, connections, and software applications
B. Defining application security standards for internally developed applications
C. Tracking and monitoring availability of vendor updates and any timelines for end of support
D. Identifying and tracking adherence to IT asset end-of-life policy

Answer: B

NEW QUESTION 71
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

NEW QUESTION 76
Which of the following is a positive aspect of adhering to a secure SDLC?

A. Promotes a ??check the box" compliance approach
B. A process that defines and meets both the business requirements and the security requirements
C. A process that forces quality code repositories management
D. Enables the process if system code is managed in different IT silos

Answer: B

NEW QUESTION 80
Which statement is FALSE regarding the different types of contracts and agreements between outsourcers and service providers?

A. Contract addendums are not sufficient for addressing third party risk obligations as each requirement must be outlined in the Master Services Agreement (MSA)
B. Evergreen contracts are automatically renewed for each party after the maturity period, unless terminated under existing contract provisions
C. Requests for Proposals (RFPs) for outsourced services should include mandatory requirements based on an organization's TPRM program policies, standards and procedures
D. Statements of Work (SOWs) define operational requirements and obligations for each party

Answer: A

NEW QUESTION 82
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

NEW QUESTION 84
Which cloud deployment model is primarily focused on the application layer?

A. Infrastructure as a Service
B. Software as a Service
C. Function a3 a Service
D. Platform as a Service

Answer: B

NEW QUESTION 88
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CTPRP Practice Exam Features:

* CTPRP Questions and Answers Updated Frequently

* CTPRP Practice Questions Verified by Expert Senior Certified Staff

* CTPRP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CTPRP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year