Shared-Assessments

Exam Questions CTPRP

Certified Third-Party Risk Professional (CTPRP)

NEW QUESTION 1
You are reviewing assessment results of workstation and endpoint security. Which result should trigger more investigation due to greater risk potential?

A. Use of multi-tenant laptops
B. Disabled printing and USB devices
C. Use of desktop virtualization
D. Disabled or blocked access to internet

Answer: A

NEW QUESTION 2
A set of principles for software development that address the top application security risks and industry web requirements is known as:

A. Application security design standards
B. Security testing methodology
C. Secure code reviews
D. Secure architecture risk analysis

Answer: A

NEW QUESTION 3
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 4
The primary disadvantage of Single Sign-On (SSO) access control is:

A. The impact of a compromise of the end-user credential that provides access to multiple systems is greater
B. A single password is easier to guess and be exploited
C. Users store multiple passwords in a single repository limiting the ability to change the password
D. Vendors must develop multiple methods to integrate system access adding cost and complexity

Answer: A

NEW QUESTION 5
You are assessing your organization's Disaster Recovery and Business Continuity (BR/BCP) requirements based on the shift to remote work. Which statement is LEAST reflective of current practices in business resiliency?

A. Third party service providers should be included in the company??s exercise and testing program based on the criticality of the outsourced business function
B. The right to require participation in testing with third party service providers should be included in the contract
C. The contract is the only enforceable control to stipulate third party service provider obligations for DR/BCP since both programs were triggered by the pandemic
D. Management should request and receive artifacts that Gemonstrate successful test results and any remediation action plans

Answer: C

NEW QUESTION 6
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 7
Which statement is FALSE regarding the methods of measuring third party risk?

A. Risk can be measured both qualitatively and quantitatively
B. Risk can be quantified by calculating the severity of impact and likelihood of occurrence
C. Assessing risk impact requires an analysis of prior events, frequency of occurrence, and external trends to analyze and predict the potential of a particular event happening
D. Risk likelihood or probability is a critical element in quantifying inherent or residual risk

Answer: C

NEW QUESTION 8

You are updating program requirements due to shift in use of technologies by vendors to enable hybrid work. Which statement is LEAST likely to represent components of an Asset Management Program?

A. Asset inventories should include connections to external parties, networks, or systems that process data
B. Each asset should include an organizational owner who is responsible for the asset throughout its life cycle
C. Assets should be classified based on criticality or data sensitivity
D. Asset inventories should track the flow or distribution of items used to fulfill products and Services across production lines

Answer: D

NEW QUESTION 9
Which of the following is NOT an example of a type of application security testing?

A. Cookie consent scanning
B. Interactive testing
C. Static testing
D. Dynamic testing

Answer: A

NEW QUESTION 10
Which statement is FALSE regarding problem or issue management?

A. Problems or issues are the root cause of an actual or potential incident
B. Problem or issue management involves managing workarounds or known errors
C. Problems or issues typically lead to systemic failures
D. Problem or issue management may reduce the likelihood and impact of incidents

Answer: C

NEW QUESTION 10
Which of the following BEST reflects the risk of a ??shadow IT" function?

A. ??Shadow IT" functions often fail to detect unauthorized use of information assets
B. ??Shadow IT" functions often lack governance and security oversight
C. inability to prevent "shadow IT?? functions from using unauthorized software solutions
D. Failure to implement strong security controls because IT is executed remotely

Answer: B

NEW QUESTION 12
Which approach for managing end-user device security is typically used for lost or stolen company-owned devices?

A. Remotely enable lost mode status on the device
B. Deletion of data after a pre-defined number of failed login attempts
C. Enterprise wipe of all company data and contacts
D. Remote wipe of the device and restore to factory settings

Answer: D

NEW QUESTION 13
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 15
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 18
Which policy requirement is typically NOT defined in an Asset Management program?

A. The Policy states requirements for the reuse of physical media (e.9., devices, servers, disk drives, etc.)

B. The Policy requires that employees and contractors return all company data and assets upon termination of their employment, contract or agreement
C. The Policy defines requirements for the inventory, identification, and disposal of equipment ??and/or physical media
D. The Policy requires visitors (including other tenants and maintenance personnel) to sign- in and sign-out of the facility, and to be escorted at all times

Answer: D

NEW QUESTION 23
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 28
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

NEW QUESTION 32
Which of the following is NOT a key component of TPRM requirements in the software development life cycle (SDLC)?

A. Maintenance of artifacts that provide proof that SOLC gates are executed
B. Process for data destruction and disposal
C. Software security testing
D. Process for fixing security defects

Answer: B

NEW QUESTION 33
Which of the following BEST reflects components of an environmental controls testing program?

A. Scheduling testing of building access and intrusion systems
B. Remote monitoring of HVAC, Smoke, Fire, Water or Power
C. Auditing the CCTV backup process and card-key access process
D. Conducting periodic reviews of personnel access controls and building intrusion systems

Answer: B

NEW QUESTION 37
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 41
Which of the following statements BEST represent the relationship between incident response and incident notification plans?

A. Cybersecurity incident response programs have the same scope and objectives as privacy incident notification procedures
B. All privacy and security incidents should be treated alike until analysis is performed to quantify the number of records impacted
C. Security incident response management is only included in crisis communication for externally reported events
D. A security incident may become a security breach based upon analysis and trigger the organization's incident notification or crisis communication process

Answer: D

NEW QUESTION 44
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 46
Upon completion of a third party assessment, a meeting should be scheduled with which of the following resources prior to sharing findings with the vendor/service provider to approve remediation plans:

A. CISO/CIO
B. Business Unit Relationship Owner
C. internal Audit
D. C&O

Answer: B

NEW QUESTION 48
Which vendor statement provides the BEST description of the concept of least privilege?

A. We require dual authorization for restricted areas
B. We grant people access to the minimum necessary to do their job
C. We require separation of duties for performance of high risk activities
D. We limit root and administrator access to only a few personnel

Answer: B

NEW QUESTION 50
Which statement is TRUE regarding defining vendor classification or risk tiering in a TPRM program?

A. Vendor classification and risk tiers are based upon residual risk calculations
B. Vendor classification and risk tiering should only be used for critical third party relationships
C. Vendor classification and corresponding risk tiers utilize the same due diligence standards for controls evaluation based upon policy
D. Vendor classification and risk tier is determined by calculating the inherent risk associated with outsourcing a specific product or service

Answer: D

NEW QUESTION 53
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 57
Which statement is NOT an example of the purpose of internal communications and information sharing using TPRM performance metrics?

A. To communicate the status of findings identified in vendor assessments and escalate issues es needed
B. To communicate the status of policy compliance with TPRM onboarding, periodic assessment and off-boarding requirements
C. To document the agreed upon corrective action plan between external parties based on the severity of findings
D. To develop and provide periodic reporting to management based on TPRM results

Answer: C

NEW QUESTION 60
Which statement is FALSE regarding background check requirements for vendors or service providers?

A. Background check requirements are not applicable for vendors or service providers based outside the United States
B. Background checks should be performed prior to employment and may be updated after employment based upon criteria in HR policies
C. Background check requirements should be applied to employees, contract workers and temporary workers
D. Background check requirements may differ based on level of authority, risk, or job role

Answer: A

NEW QUESTION 65
.....

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