Shared-Assessments

Exam Questions CTPRP

Certified Third-Party Risk Professional (CTPRP)

NEW QUESTION 1
Which activity BEST describes conducting due diligence of a lower risk vendor?

A. Accepting a service providers self-assessment questionnaire responses
B. Preparing reports to management regarding the status of third party risk management and remediation activities
C. Reviewing a service provider's self-assessment questionnaire and external audit report(s)
D. Requesting and filing a service provider's external audit report(s) for future reference

Answer: A

NEW QUESTION 2
When working with third parties, which of the following requirements does not reflect a ??Zero Trust" approach to access management?

A. Utilizing a solution that allows direct access by third parties to the organization's network
B. Ensure that access is granted on a per session basis regardless of network location, user, or device
C. Implement device monitoring, continual inspection and monitoring of logs/traffic
D. Require that all communication is secured regardless of network location

Answer: A

NEW QUESTION 3
Which statement BEST describes the methods of performing due diligence during third party risk assessments?

A. Inspecting physical and environmental security controls by conducting a facility tour
B. Reviewing status of findings from the questionnaire and defining remediation plans
C. interviewing subject matter experts or control owners, reviewing compliance artifacts, and validating controls
D. Reviewing and assessing only the obligations that are specifically defined in the contract

Answer: C

NEW QUESTION 4
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 5
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 6
Which of the following methods of validating pre-employment screening attributes is appropriate due to limitations of international or state regulation?

A. Reviewing evidence of web search of social media sites
B. Providing and sampling complete personnel files to demonstrate unique screeningresults
C. Requiring evidence of drug testing
D. Requesting evidence of the performance of pre-employment screening when permitted by law

Answer: D

NEW QUESTION 7
The BEST way to manage Fourth-Nth Party risk is:

A. Include a provision in the vender contract requiring the vendor to provide notice and obtain written consent before outsourcing any service
B. Include a provision in the contract prohibiting the vendor from outsourcing any service which includes access to confidential data or systems
C. Incorporate notification and approval contract provisions for subcontracting that require evidence of due diligence as defined by a TPRM program
D. Require the vendor to maintain a cyber-insurance policy for any service that is outsourced which includes access to confidential data or systems

Answer: C

NEW QUESTION 8
Which of the following factors is MOST important when assessing the risk of shadow IT in organizational security?

A. The organization maintains adequate policies and procedures that communicate required controls for security functions
B. The organization requires security training and certification for security personnel
C. The organization defines staffing levels to address impact of any turnover in security roles
D. The organization's resources and investment are sufficient to meet security requirements

Answer: A

NEW QUESTION 9
Which requirement is the MOST important for managing risk when the vendor contract terminates?

A. The responsibility to perform a financial review of outstanding invoices
B. The commitment to perform a final assessment based upon due diligence standards
C. The requirement to ensure secure data destruction and asset return
D. The obligation to define contract terms for transition services

Answer: C

NEW QUESTION 10
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 10
Which risk treatment approach typically requires a negotiation of contract terms between parties?

A. Monitor the risk
B. Mitigate the risk
C. Accept the risk
D. Transfer the risk

Answer: D

NEW QUESTION 15
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 18
When conducting an assessment of a third party's physical security controls, which of the following represents the innermost layer in a ??Defense in Depth?? model?

A. Public internal
B. Restricted entry
C. Private internal
D. Public external

Answer: C

NEW QUESTION 19
Which of the following actions reflects the first step in developing an emergency response plan?

A. Conduct an assessment that includes an inventory of the types of events that have the greatest potential to trigger an emergency response plan
B. Consider work-from-home parameters in the emergency response plan
C. incorporate periodic crisis management team tabletop exercises to test different scenarios
D. Use the results of continuous monitoring tools to develop the emergency response plan

Answer: A

NEW QUESTION 22
Which statement provides the BEST example of the purpose of scoping in third party assessments?

A. Scoping is used to reduce the number of questions the vendor has to complete based on vendor ??classification
B. Scoping is the process an outsourcer uses to configure a third party assessment based on the risk the vendor presents to the organization
C. Scoping is an assessment technique only used for high risk or critical vendors that require on-site assessments
D. Scoping is used primarily to limit the inclusion of supply chain vendors in third party assessments

Answer: B

NEW QUESTION 25
Which statement is TRUE regarding the use of questionnaires in third party risk assessments?

A. The total number of questions included in the questionnaire assigns the risk tier
B. Questionnaires are optional since reliance on contract terms is a sufficient control
C. Assessment questionnaires should be configured based on the risk rating and type of service being evaluated
D. All topic areas included in the questionnaire require validation during the assessment

Answer: C

NEW QUESTION 26
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 28
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 31
Minimum risk assessment standards for third party due diligence should be:

A. Set by each business unit based on the number of vendors to be assessed
B. Defined in the vendor/service provider contract or statement of work
C. Established by the TPRM program based on the company??s risk tolerance and risk appetite
D. Identified by procurement and required for all vendors and suppliers

Answer: C

NEW QUESTION 36
You are updating the inventory of regulations that impact your TPRM program during the company's annual risk assessment. Which statement provides the optimal approach to prioritizing the regulations?

A. identify the applicable regulations that require an extension of specific obligations to service providers
B. Narrow the focus only on the regulations that directly apply to personal information
C. Include the regulations that have the greater risk of triggering enforcement or fines/penalties
D. Emphasize the federal regulations since they supersede state regulations

Answer: A

NEW QUESTION 40
Which activity reflects the concept of vendor management?

A. Managing service level agreements
B. Scanning and collecting information from third party web sites
C. Reviewing and analyzing external audit reports
D. Receiving and analyzing a vendor's response to & questionnaire

Answer: A

NEW QUESTION 42
Physical access procedures and activity logs should require all of the following EXCEPT:

A. Require multiple access controls for server rooms and data centers
B. Require physical access logs to be retained indefinitely for audit purposes
C. Record successful and unsuccessful attempts including investigation of unsuccessful access attempts
D. Include a process to trigger review of the logs after security events

Answer: B

NEW QUESTION 43

Which of the following is NOT an attribute in the vendor inventory used to assign risk rating and vendor classification?

A. Type of data accessed, processed, or retained
B. Type of systems accessed
C. Type of contract addendum
D. Type of network connectivity

Answer: C

NEW QUESTION 44
Which statement does NOT reflect current practice in addressing fourth party risk or subcontracting risk?

A. Third party contracts and agreements should require prior notice and approval for subcontracting
B. Outsourcers should rely on requesting and reviewing external audit reports to address subcontracting risk
C. Outsourcers should inspect the vendor's TPRM program and require evidence of the assessments of subcontractors
D. Third party contracts should include capturing, maintaining, and tracking authorized subcontractors

Answer: B

NEW QUESTION 46
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 50
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 51
A visual representation of locations, users, systems and transfer of personal information between outsourcers and third parties is defined as:

A. Configuration standard
B. Audit log report
C. Network diagram
D. Data flow diagram

Answer: D

NEW QUESTION 54
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 59
Which example of a response to external environmental factors is LEAST likely to be managed directly within the BCP or IT DR plan?

A. Protocols for social media channels and PR communication
B. Response to a natural or man-made disruption
C. Dependency on key employee or supplier issues
D. Response to a large scale illness or health outbreak

Answer: A

NEW QUESTION 61
Your company has been alerted that an IT vendor began utilizing a subcontractor located in a country restricted by company policy. What is the BEST approach to handle this situation?

A. Notify management to approve an exception and ensure that contract provisions require prior ??notification and evidence of subcontractor due diligence
B. inform the business unit and recommend that the company cease future work with the IT vendor due to company policy

C. Update the vender inventory with the mew location information in order to schedule a reassessment
D. Inform the business unit and ask the vendor to replace the subcontractor at their expense in ??order to move the processing back to an approved country

Answer: D

NEW QUESTION 64
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 66
Which statement is TRUE regarding the onboarding process far new hires?

A. New employees and contractors should not be on-boarded until the results of applicant screening are approved
B. it is not necessary to have employees, contractors, and third party users sign confidentiality or non-disclosure agreements
C. All job roles should require employees to sign non-compete agreements
D. New employees and contactors can opt-out of having to attend security and privacy awareness training if they hold existing certifications

Answer: A

NEW QUESTION 68
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 73
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 74
The BEST time in the SDLC process for an application service provider to perform Threat Modeling analysis is:

A. Before the application design and development activities begin
B. After the application vulnerability or penetration test is completed
C. After testing and before the deployment of the final code into production
D. Prior to the execution of a contract with each client

Answer: A

NEW QUESTION 79
Which capability is LEAST likely to be included in the annual testing activities for Business Continuity or Disaster Recovery plans?

A. Plans to enable technology and business operations to be resumed at a back-up site
B. Process to validate that specific databases can be accessed by applications at the designated location
C. Ability for business personnel to perform their functions at an alternate work space location
D. Require participation by third party service providers in collaboration with industry exercises

Answer: D

NEW QUESTION 84
When evaluating remote access risk, which of the following is LEAST applicable to your analysis?

A. Logging of remote access authentication attempts
B. Limiting access by job role of business justification
C. Monitoring device activity usage volumes
D. Requiring application whitelisting

Answer: D

NEW QUESTION 86
An IT change management approval process includes all of the following components EXCEPT:

A. Application version control standards for software release updates
B. Documented audit trail for all emergency changes
C. Defined roles between business and IT functions
D. Guidelines that restrict approval of changes to only authorized personnel

Answer: A

NEW QUESTION 91
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 94
Which statement reflects a requirement that is NOT typically found in a formal Information Security Incident Management Program?

A. The program includes the definition of internal escalation processes
B. The program includes protocols for disclosure of information to external parties
C. The program includes mechanisms for notification to clients
D. The program includes processes in support of disaster recovery

Answer: D

NEW QUESTION 99
During the contract negotiation process for a new vendor, the vendor states they have legal obligations to retain data for tax purposes. However, your company policy requires data return or destruction at contract termination. Which statement provides the BEST approach to address this conflict?

A. Determine if a policy exception and approval is required, and require that data safeguarding obligations continue after termination
B. Change the risk rating of the vendor to reflect a higher risk tier
C. Insist the vendor adheres to the policy and contract provisions without exception
D. Conduct an assessment of the vendor's data governance and records management program

Answer: A

NEW QUESTION 103
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 108
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 111
In which phase of the TPRM lifecycle should terms for return or destruction of data be defined and agreed upon?

A. During contract negotiation
B. At third party selection and initial due diligence
C. When deploying ongoing monitoring
D. At termination and exit

Answer: A

NEW QUESTION 115
.....

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