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
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 3
Tracking breach, credential exposure and insider fraud/theft alerts is an example of which continuous monitoring technique?

A. Monitoring surface
B. Vulnerabilities
C. Passive and active indicators of compromise
D. Business intelligence

Answer: C

NEW QUESTION 4
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 5
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 6
Which of the following components is NOT typically included in external continuous monitoring solutions?

A. Status updates on localized events based on geolocation
B. Alerts on legal and regulatory actions involving the vendor
C. Metrics that track SLAs for performance management
D. Reports that identify changes in vendor financial viability

Answer: C

NEW QUESTION 7
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 8
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 9
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

NEW QUESTION 10
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 10
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 12
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 13
Which of the following data types would be classified as low risk data?

A. Sanitized customer data used for aggregated profiling
B. Non personally identifiable, but sensitive to an organizations significant process
C. Government-issued number, credit card number or bank account information
D. Personally identifiable data but stored in a test environment cloud container

Answer: A

NEW QUESTION 15
Which of the following BEST describes the distinction between a regulation and a standard?

A. A regulation must be adhered to by all companies subject to its requirements, but companies ??can voluntarily choose to follow standards.
B. There is no distinction, regulations and standards are the same and have equal impact
C. Standards are always a subset of a regulation
D. A standard must be adhered to by companies based on the industry they are in, while regulations are voluntary.

Answer: A

NEW QUESTION 19
Select the risk type that is defined as: ??A third party may not be able to meet its obligations due to inadequate systems or processes??.

A. Reliability risk
B. Performance risk
C. Competency risk
D. Availability risk

Answer: B

NEW QUESTION 21
Which type of contract termination is MOST likely to occur after failure to remediate assessment findings?

A. Regulatory/supervisory termination
B. Termination for convenience
C. Normal termination
D. Termination for cause

Answer: D

NEW QUESTION 23
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 27
Which statement is FALSE regarding analyzing results from a vendor risk assessment?

A. The frequency for conducting a vendor reassessment is defined by regulatory obligations
B. Findings from a vendor risk assessment may be defined at the entity level, and are based o na Specific topic or control
C. Identifying findings from a vendor risk assessment can occur at any stage in the contract lifecycle
D. Risk assessment findings identified by controls testing or validation should map back to the information gathering questionnaire and agreed upon framework

Answer: A

NEW QUESTION 30
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 31
Which statement BEST describes the use of risk based decisioning in prioritizing gaps identified at a critical vendor when defining the corrective action plan?

A. The assessor determined that gaps should be analyzed, documented, reviewed for compensating controls, and submitted to the business owner to approve risk treatment plan
B. The assessor decided that the critical gaps should be discussed in the closing meeting so that the vendor can begin to implement corrective actions immediately
C. The assessor concluded that all gaps should be logged and treated as high severity findings since the assessment was performed on a critical vendor
D. The assessor determined that all gaps should be logged and communicated that if the gaps were corrected immediately they would not need to be included in the findings report

Answer: A

NEW QUESTION 33
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 34
Which requirement is NOT included in IT asset end-of-life (EOL) processes?

A. The requirement to conduct periodic risk assessments to determine end-of-life
B. The requirement to track status using a change initiation request form
C. The requirement to track updates to third party provided systems or applications for any planned end-of-life support
D. The requirement to establish defined procedures for secure destruction al sunset of asset

Answer: A

NEW QUESTION 35
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 39
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 41
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 45
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 48
Which statement is FALSE regarding the risk factors an organization may include when defining TPRM compliance requirements?

A. Organizations include TPRM compliance requirements within vendor contracts, and periodically review and update mandatory contract provisions
B. Organizations rely on regulatory mandates to define and structure TPRM compliance requirements
C. Organizations incorporate the use of external standards and frameworks to align and map TPRM compliance requirements to industry practice
D. Organizations define TPRM policies based on the company??s risk appetite to shape requirements based on the services being outsourced

Answer: B

NEW QUESTION 51
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 53
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 54
Which statement BEST represents the roles and responsibilities for managing corrective actions upon completion of an onsite or virtual assessment?

A. All findings and remediation plans should be reviewed with internal audit prior to issuing the assessment report

B. All findings and remediation plans should be reviewed with the vendor prior to sharing results with the line of business
C. All findings and need for remediation should be reviewed with the line of business for risk acceptance prior to sharing the remediation plan with the vendor
D. All findings should be shared with the vendor as quickly as possible so that remediation steps can be taken as quickly as possible

Answer: C

NEW QUESTION 59
Once a vendor questionnaire is received from a vendor what is the MOST important next step when evaluating the responses?

A. Document your analysis and provide confirmation to the business unit regarding receipt of the questionnaire
B. Update the vender risk registry and vendor inventory with the results in order to complete the assessment
C. Calculate the total number of findings to rate the effectiveness of the vendor response
D. Analyze the responses to identify adverse or high priority responses to prioritize controls that should be tested

Answer: D

NEW QUESTION 64
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 67
Which statement is FALSE when describing the third party risk assessors?? role when conducting a controls evaluation using an industry framework?

A. The Assessor's role is to conduct discovery with subject matter experts to understand the control environment
B. The Assessor's role is to conduct discovery and validate responses from the risk assessment questionnaire by testing or validating controls
C. The Assessor's role is to provide an opinion on the effectiveness of controls conducted over a period of time in their report
D. The Assessor's role is to review compliance artifacts and identify potential control gaps based on evaluation of the presence of control attributes

Answer: C

NEW QUESTION 72
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 75
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 76
Which statement is NOT an accurate reflection of an organizations requirements within an enterprise information security policy?

A. Security policies should define the organizational structure and accountabilities for oversight
B. Security policies should have an effective date and date of last review by management
C. Security policies should be changed on an annual basis due to technology changes
D. Security policies should be organized based upon an accepted control framework

Answer: C

NEW QUESTION 77
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 82
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 86
Which of the following is a component of evaluating a third party's use of Remote Access within their information security policy?

A. Maintaining blocked IP address ranges
B. Reviewing the testing and deployment procedures to networking components
C. Providing guidelines to configuring ports on a router
D. Identifying the use of multifactor authentication

Answer: D

NEW QUESTION 90
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 94
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 99
Which statement is TRUE regarding the tools used in TPRM risk analyses?

A. Risk treatment plans define the due diligence standards for third party assessments
B. Risk ratings summarize the findings in vendor remediation plans
C. Vendor inventories provide an up-to-date record of high risk relationships across an organization
D. Risk registers are used for logging and tracking third party risks

Answer: D

NEW QUESTION 102
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 107
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 111
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 114
Which approach demonstrates GREATER maturity of physical security compliance?

A. Leveraging periodic reporting to schedule facility inspections based on reported events
B. Providing a checklist for self-assessment
C. Maintaining a standardized scheduled for confirming controls to defined standards
D. Conducting unannounced checks an an ac-hac basis

Answer: C

NEW QUESTION 119
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 124
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 125
Which example is typically NOT included in a Business Impact Analysis (BIA)?

A. Including any contractual or legal/regulatory requirements
B. Prioritization of business functions and processes
C. Identifying the criticality of applications
D. Requiring vendor participation in testing

Answer: D

NEW QUESTION 129
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 133
Which TPRM risk assessment component would typically NOT be maintained in a Risk Register?

A. An assessment of the impact and likelihood the risk will occur and the possible seriousness
B. Vendor inventory of all suppliers, vendors, and service providers prioritized by contract value
C. An outline of proposed mitigation actions and assignment of risk owner
D. A grading of each risk according to a risk assessment table or hierarchy

Answer: B

NEW QUESTION 136
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 138
Which type of external event does NOT trigger an organization ta prompt a third party contract provisions review?

A. Change in company point of contact
B. Business continuity event
C. Data breach/privacy incident
D. Change in regulations

Answer: A

NEW QUESTION 142
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 147
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 152
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 155
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 159
When defining due diligence requirements for the set of vendors that host web applications which of the following is typically NOT part of evaluating the vendor's patch management controls?

A. The capability of the vendor to apply priority patching of high-risk systems
B. Established procedures for testing of patches, service packs, and hot fixes prior to installation
C. A documented process to gain approvals for use of open source applications
D. The existence of a formal process for evaluation and prioritization of known vulnerabilities

Answer: C

NEW QUESTION 160
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

NEW QUESTION 164

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 166
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 169
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 170
.....

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