Shared-Assessments

Exam Questions CTPRP

Certified Third-Party Risk Professional (CTPRP)

NEW QUESTION 1
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 2
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 3
Which example BEST represents the set of restrictive areas that require an additional authentication factor for access control?

A. Datacenters; telecom rooms; server rooms; exterior building entrance
B. Datacenters; telecom rooms; security operations centers; loading docks
C. Telecom rooms; parking garage; security operations centers; exterior building entrance
D. Exterior building entrance; datacenters; telecom rooms; printer rooms

Answer: A

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
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 6
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 7
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 8
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 9
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 10
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 10
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 12
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 14
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 15
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 16
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 20
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 22
Which statement is TRUE regarding a vendor's approach to Environmental, Social, and Governance (ESG) programs?

A. ESG expectations are driven by a company's executive team for internal commitments end not external entities
B. ESG requirements and programs may be directed by regulatory obligations or in response to company commitments
C. ESG commitments can only be measured qualitatively so it cannot be included in vendor due diligence standards
D. ESG obligations only apply to a company with publicly traded stocks

Answer: B

NEW QUESTION 24
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 25
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 26
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 27
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 32
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 37
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 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 42
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 44
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 48
Which of the following statements is TRUE regarding the accountabilities in a three lines of defense model?

A. The second line of defense is management within the business unit
B. The first line of defense is the risk or compliance team that provides an oversight or governance function
C. The third line of defense is an assurance function that has independence from the business unit
D. The third line of defense must be limited to an external assessment firm

Answer: C

NEW QUESTION 50
Which cloud deployment model is focused on the management of hardware equipment?

A. Function as a service
B. Platform as a service
C. Software as a service
D. Infrastructure as a service

Answer: D

NEW QUESTION 51
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 54
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 56
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 61
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 62
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 65
What attribute is MOST likely to be included in the software development lifecycle (SDLC) process?

A. Scheduling the frequency of automated vulnerability scans
B. Scanning for data input validation in production
C. Conducting peer code reviews
D. Defining the scope of annual penetration tests

Answer: C

NEW QUESTION 70
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 71
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 72
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 76

.....

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