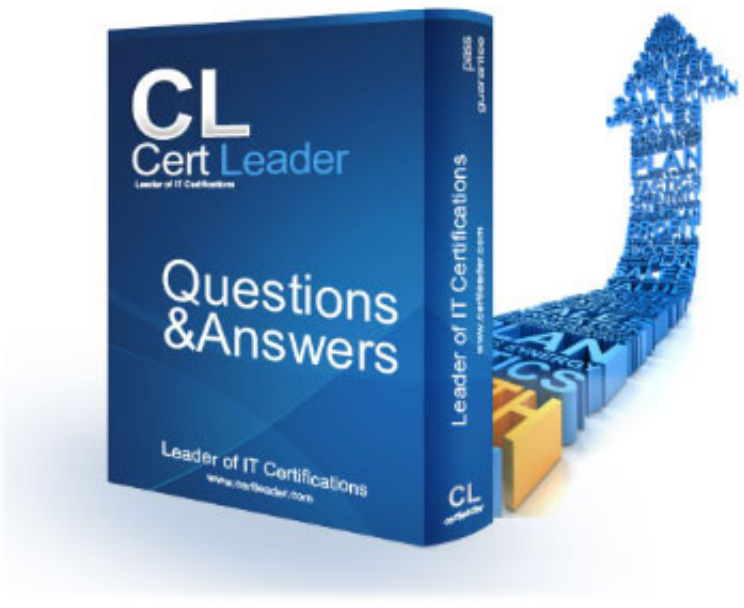
CTPRP Dumps

Certified Third-Party Risk Professional (CTPRP)

https://www.certleader.com/CTPRP-dumps.html



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 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 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 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 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 7
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 8
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 9
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 10
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 10
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 14
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 16
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 19
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 20
When defining third party requirements for transmitting Pll, which factors provide stranger controls?

A. Full disk encryption and backup
B. Available bandwidth and redundancy
C. Strength of encryption cipher and authentication method

D. Logging and monitoring

Answer: C

NEW QUESTION 21
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 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 30
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 31
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 35
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 39
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 44
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 48
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 53
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 57
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 60
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 64
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 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 72
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 73
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 76
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 79
All of the following processes are components of controls evaluation in the Third Party Risk Assessment process EXCEPT:

A. Reviewing compliance artifacts for the presence of control attributes
B. Negotiating contract terms for the right to audit
C. Analyzing assessment results to identify and report risk
D. Scoping the assessment based on identified risk factors

Answer: B

NEW QUESTION 80
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 83
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CTPRP Exam with Our Prep Materials Via below:

https://www.certleader.com/CTPRP-dumps.html