Shared-Assessments

Exam Questions CTPRP

Certified Third-Party Risk Professional (CTPRP)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
Which statement is TRUE regarding artifacts reviewed when assessing the Cardholder Data Environment (CDE) in payment card processing?

A. The Data Security Standards (DSS) framework should be used to scope the assessment
B. The Report on Compliance (ROC) provides the assessment results completed by a qualified security assessor that includes an onsite audit
C. The Self-Assessment Questionnaire (SAQ) provides independent testing of controls
D. A System and Organization Controls (SOC) report is sufficient if the report addresses the same location

Answer: B

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
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 6
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 7
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 8
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 9
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 10
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 10
Which set of procedures is typically NOT addressed within data privacy policies?

A. Procedures to limit access and disclosure of personal information to third parties
B. Procedures for handling data access requests from individuals
C. Procedures for configuration settings in identity access management
D. Procedures for incident reporting and notification

Answer: C

NEW QUESTION 14
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 15
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 18
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 NOT a method of securing web applications?

A. Ensure appropriate logging and review of access and events
B. Conduct periodic penetration tests
C. Adhere to web content accessibility guidelines
D. Include validation checks in SDLC for cross site scripting and SOL injections

Answer: C

NEW QUESTION 21
When defining third party requirements for transmitting PII, 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 24
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 28
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 31
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 32
Which statement is FALSE regarding the foundational requirements of a well-defined third party risk management program?

A. We conduct onsite or virtual assessments for all third parties
B. We have defined senior and executive management accountabilities for oversight of our TPRM program
C. We have established vendor risk ratings and classifications based on a tiered hierarchy
D. We have established Management and Board-level reporting to enable risk-based decisionmaking

Answer: A

NEW QUESTION 36
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 37
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 41

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 43
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 47
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 50
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 51
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 55
You receive a call from a vendor that two laptops and a tablet are missing that were used to process your company data. The asset loss occurred two years ago, but was only recently discovered. That statement may indicate that this vendor is lacking an adequate:

A. Asset Management Program
B. Physical and Environmental Security Program
C. Data Loss Prevention Program
D. Information Security Incident Notification Policy

Answer: A

NEW QUESTION 59
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 63
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 68
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 71
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 73
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 74
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. APl integration

Answer: B

NEW QUESTION 78
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 79
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 81
Which factor is the LEAST important attribute when classifying personal data?

A. The volume of data records processed or retained
B. The data subject category that identifies the data owner
C. The sensitivity level of specific data elements that could identify an individual
D. The assignment of a confidentiality level that differentiates public or non-public information

Answer: A

NEW QUESTION 84
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 88
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 91
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 92
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 93
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 97
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 99
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 104
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 108
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 113
.....

Relate Links

100% Pass Your CTPRP Exam with Exambible Prep Materials

https://www.exambible.com/CTPRP-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/