Shared-Assessments

Exam Questions CTPRP

Certified Third-Party Risk Professional (CTPRP)

NEW QUESTION 1
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 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
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 13
You are assessing your organization's Disaster Recovery and Business Continuity (BR/BCP) requirements based on the shift to remote work. Which statement is LEAST reflective of current practices in business resiliency?

A. Third party service providers should be included in the company??s exercise and testing program based on the criticality of the outsourced business function
B. The right to require participation in testing with third party service providers should be included in the contract
C. The contract is the only enforceable control to stipulate third party service provider obligations for DR/BCP since both programs were triggered by the pandemic
D. Management should request and receive artifacts that Gemonstrate successful test results and any remediation action plans

Answer: C

NEW QUESTION 17
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 18
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 20
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 22
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 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 26
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 31
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 32
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 37
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 39
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 44
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 48
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 51
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 54
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 55
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 60
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 65
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 69
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 71
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 73
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 74
Which factor describes the concept of criticality of a service provider relationship when determining vendor classification?

A. Criticality is limited to only the set of vendors involved in providing disaster recovery services
B. Criticality is determined as all high risk vendors with access to personal information
C. Criticality is assigned to the subset of vendor relationships that pose the greatest impact due to their unavailability
D. Criticality is described as the set of vendors with remote access or network connectivity to company systems

Answer: C

NEW QUESTION 75
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 80
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 81
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 82
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 84
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 85
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 88
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 89
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 93
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 96
Which statement is TRUE regarding defining vendor classification or risk tiering in a TPRM program?

A. Vendor classification and risk tiers are based upon residual risk calculations
B. Vendor classification and risk tiering should only be used for critical third party relationships
C. Vendor classification and corresponding risk tiers utilize the same due diligence standards for controls evaluation based upon policy
D. Vendor classification and risk tier is determined by calculating the inherent risk associated with outsourcing a specific product or service

Answer: D

NEW QUESTION 98
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 99
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 103
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 106
.....

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