

Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control



NEW QUESTION 1

- (Exam Topic 4)

When developing a response plan to address security incidents regarding sensitive data loss, it is MOST important

- A. revalidate current key risk indicators (KRIs).
- B. revise risk management procedures.
- C. review the data classification policy.
- D. revalidate existing risk scenarios.

Answer: C

NEW QUESTION 2

- (Exam Topic 4)

A global company's business continuity plan (BCP) requires the transfer of its customer information.... event of a disaster. Which of the following should be the MOST important risk consideration?

- A. The difference in the management practices between each company
- B. The cloud computing environment is shared with another company
- C. The lack of a service level agreement (SLA) in the vendor contract
- D. The organizational culture differences between each country

Answer: B

NEW QUESTION 3

- (Exam Topic 4)

A highly regulated enterprise is developing a new risk management plan to specifically address legal and regulatory risk scenarios. What should be done FIRST by IT governance to support this effort?

- A. Request a regulatory risk reporting methodology
- B. Require critical success factors (CSFs) for IT risks.
- C. Establish IT-specific compliance objectives
- D. Communicate IT key risk indicators (KRIs) and triggers

Answer: A

NEW QUESTION 4

- (Exam Topic 4)

Which of the following is the PRIMARY accountability for a control owner?

- A. Communicate risk to senior management.
- B. Own the associated risk the control is mitigating.
- C. Ensure the control operates effectively.
- D. Identify and assess control weaknesses.

Answer: C

NEW QUESTION 5

- (Exam Topic 4)

An organization has decided to postpone the assessment and treatment of several risk scenarios because stakeholders are unavailable. As a result of this decision, the risk associated with these new entries has been;

- A. mitigated
- B. deferred
- C. accepted.
- D. transferred

Answer: C

NEW QUESTION 6

- (Exam Topic 4)

Which of the following would provide the MOST useful input when evaluating the appropriateness of risk responses?

- A. Incident reports
- B. Cost-benefit analysis
- C. Risk tolerance
- D. Control objectives

Answer: B

NEW QUESTION 7

- (Exam Topic 4)

A poster has been displayed in a data center that reads, "Anyone caught taking photographs in the data center may be subject to disciplinary action." Which of the following control types has been implemented?

- A. Corrective

- B. Detective
- C. Deterrent
- D. Preventative

Answer: A

NEW QUESTION 8

- (Exam Topic 4)

Using key risk indicators (KRIs) to illustrate changes in the risk profile PRIMARILY helps to:

- A. communicate risk trends to stakeholders.
- B. assign ownership of emerging risk scenarios.
- C. highlight noncompliance with the risk policy
- D. identify threats to emerging technologies.

Answer: A

NEW QUESTION 9

- (Exam Topic 4)

When a risk practitioner is determining a system's criticality, it is MOST helpful to review the associated:

- A. process flow.
- B. business impact analysis (BIA).
- C. service level agreement (SLA).
- D. system architecture.

Answer: B

NEW QUESTION 10

- (Exam Topic 4)

Risk appetite should be PRIMARILY driven by which of the following?

- A. Enterprise security architecture roadmap
- B. Stakeholder requirements
- C. Legal and regulatory requirements
- D. Business impact analysis (BIA)

Answer: B

NEW QUESTION 10

- (Exam Topic 4)

An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

- A. Threat
- B. Risk
- C. Vulnerability
- D. Policy violation

Answer: B

NEW QUESTION 11

- (Exam Topic 4)

Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

- A. The program has not decreased threat counts.
- B. The program has not considered business impact.
- C. The program has been significantly revised
- D. The program uses non-customized training modules.

Answer: D

NEW QUESTION 16

- (Exam Topic 4)

An organization is considering outsourcing user administration controls for a critical system. The potential vendor has offered to perform quarterly sett-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to me risk practitioner?

- A. The controls may not be properly tested
- B. The vendor will not ensure against control failure
- C. The vendor will not achieve best practices
- D. Lack of a risk-based approach to access control

Answer: D

NEW QUESTION 20

- (Exam Topic 4)

Which of the following would be of MOST concern to a risk practitioner reviewing risk action plans for documented IT risk scenarios?

- A. Individuals outside IT are managing action plans for the risk scenarios.
- B. Target dates for completion are missing from some action plans.
- C. Senior management approved multiple changes to several action plans.
- D. Many action plans were discontinued after senior management accepted the risk.

Answer: B

NEW QUESTION 24

- (Exam Topic 4)

Which of the following roles should be assigned accountability for monitoring risk levels?

- A. Risk practitioner
- B. Business manager
- C. Risk owner
- D. Control owner

Answer: C

NEW QUESTION 25

- (Exam Topic 4)

Which of the following provides the MOST useful information for developing key risk indicators (KRIs)?

- A. Business impact analysis (BIA) results
- B. Risk scenario ownership
- C. Risk thresholds
- D. Possible causes of materialized risk

Answer: C

NEW QUESTION 30

- (Exam Topic 4)

A core data center went offline abruptly for several hours affecting many transactions across multiple locations. Which of the following would provide the MOST useful information to determine mitigating controls?

- A. Forensic analysis
- B. Risk assessment
- C. Root cause analysis
- D. Business impact analysis (BIA)

Answer: A

NEW QUESTION 35

- (Exam Topic 4)

Which component of a software inventory BEST enables the identification and mitigation of known vulnerabilities?

- A. Software version
- B. Assigned software manager
- C. Software support contract expiration
- D. Software licensing information

Answer: A

NEW QUESTION 40

- (Exam Topic 4)

Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?

- A. A decrease in the number of critical assets covered by risk thresholds
- B. An increase in the number of risk threshold exceptions
- C. An increase in the number of change events pending management review
- D. A decrease in the number of key performance indicators (KPIs)

Answer: B

NEW QUESTION 42

- (Exam Topic 4)

Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

- A. Percentage of IT systems recovered within the mean time to restore (MTTR) during the disaster recovery test
- B. Percentage of issues arising from the disaster recovery test resolved on time
- C. Percentage of IT systems included in the disaster recovery test scope
- D. Percentage of IT systems meeting the recovery time objective (RTO) during the disaster recovery test

Answer: D

NEW QUESTION 44

- (Exam Topic 4)

A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

- A. risk score
- B. risk impact
- C. risk response
- D. risk likelihood.

Answer: B

NEW QUESTION 49

- (Exam Topic 4)

Which of the following would provide the BEST evidence of an effective internal control environment/?

- A. Risk assessment results
- B. Adherence to governing policies
- C. Regular stakeholder briefings
- D. Independent audit results

Answer: D

NEW QUESTION 50

- (Exam Topic 4)

Which of the following is MOST important to determine when assessing the potential risk exposure of a loss event involving personal data?

- A. The cost associated with incident response activitiesThe composition and number of records in the information asset
- B. The maximum levels of applicable regulatory fines
- C. The length of time between identification and containment of the incident

Answer: C

NEW QUESTION 53

- (Exam Topic 4)

A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?

- A. Collaborate with the risk owner to determine the risk response plan.
- B. Document the gap in the risk register and report to senior management.
- C. Include a right to audit clause in the service provider contract.
- D. Advise the risk owner to accept the risk.

Answer: C

NEW QUESTION 55

- (Exam Topic 3)

Which of the following BEST measures the impact of business interruptions caused by an IT service outage?

- A. Sustained financial loss
- B. Cost of remediation efforts
- C. Duration of service outage
- D. Average time to recovery

Answer: A

NEW QUESTION 57

- (Exam Topic 3)

The PRIMARY reason for prioritizing risk scenarios is to:

- A. provide an enterprise-wide view of risk
- B. support risk response tracking
- C. assign risk ownership
- D. facilitate risk response decisions.

Answer: D

NEW QUESTION 59

- (Exam Topic 4)

Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?

- A. Updating the organizational policy for remote access
- B. Creating metrics to track remote connections
- C. Implementing multi-factor authentication
- D. Updating remote desktop software

Answer: A

NEW QUESTION 63

- (Exam Topic 4)

Which of the following is MOST important to consider before determining a response to a vulnerability?

- A. The likelihood and impact of threat events
- B. The cost to implement the risk response
- C. Lack of data to measure threat events
- D. Monetary value of the asset

Answer: C

NEW QUESTION 67

- (Exam Topic 3)

Which of the following statements describes the relationship between key risk indicators (KRIs) and key control indicators (KCIs)?

- A. KRI design must precede definition of KCIs.
- B. KCIs and KRIs are independent indicators and do not impact each other.
- C. A decreasing trend of KRI readings will lead to changes to KCIs.
- D. Both KRIs and KCIs provide insight to potential changes in the level of risk.

Answer: A

NEW QUESTION 71

- (Exam Topic 3)

The BEST way to improve a risk register is to ensure the register:

- A. is updated based upon significant events.
- B. documents possible countermeasures.
- C. contains the risk assessment completion date.
- D. is regularly audited.

Answer: A

NEW QUESTION 74

- (Exam Topic 3)

Which of the following is the MOST effective control to maintain the integrity of system configuration files?

- A. Recording changes to configuration files
- B. Implementing automated vulnerability scanning
- C. Restricting access to configuration documentation
- D. Monitoring against the configuration standard

Answer: D

NEW QUESTION 75

- (Exam Topic 3)

Which of the following is the BEST way to determine the potential organizational impact of emerging privacy regulations?

- A. Evaluate the security architecture maturity.
- B. Map the new requirements to the existing control framework.
- C. Charter a privacy steering committee.
- D. Conduct a privacy impact assessment (PIA).

Answer: D

NEW QUESTION 78

- (Exam Topic 3)

Which of the following is MOST useful when communicating risk to management?

- A. Risk policy
- B. Audit report
- C. Risk map
- D. Maturity model

Answer: C

NEW QUESTION 80

- (Exam Topic 3)

A violation of segregation of duties is when the same:

- A. user requests and tests the change prior to production.
- B. user authorizes and monitors the change post-implementation.
- C. programmer requests and tests the change prior to production.
- D. programmer writes and promotes code into production.

Answer:

D

NEW QUESTION 82

- (Exam Topic 3)

The MAIN reason for creating and maintaining a risk register is to:

- A. assess effectiveness of different projects.
- B. define the risk assessment methodology.
- C. ensure assets have low residual risk.
- D. account for identified key risk factors.

Answer: D

NEW QUESTION 83

- (Exam Topic 3)

Which of the following is MOST helpful in preventing risk events from materializing?

- A. Prioritizing and tracking issues
- B. Establishing key risk indicators (KRIs)
- C. Reviewing and analyzing security incidents
- D. Maintaining the risk register

Answer: A

NEW QUESTION 84

- (Exam Topic 3)

Which of the following should be considered when selecting a risk response?

- A. Risk scenarios analysis
- B. Risk response costs
- C. Risk factor awareness
- D. Risk factor identification

Answer: B

NEW QUESTION 86

- (Exam Topic 3)

Which of the following should be the FIRST consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected?

- A. Informed consent
- B. Cross border controls
- C. Business impact analysis (BIA)
- D. Data breach protection

Answer: A

NEW QUESTION 91

- (Exam Topic 3)

The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:

- A. the proposed controls are implemented as scheduled.
- B. security controls are tested prior to implementation.
- C. compliance with corporate policies.
- D. the risk response strategy has been decided.

Answer: A

NEW QUESTION 96

- (Exam Topic 3)

A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

- A. better understands the system architecture.
- B. is more objective than risk management.
- C. can balance technical and business risk.
- D. can make better-informed business decisions.

Answer: D

NEW QUESTION 98

- (Exam Topic 3)

An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

- A. Potential increase in regulatory scrutiny
- B. Potential system downtime
- C. Potential theft of personal information

D. Potential legal risk

Answer: C

NEW QUESTION 100

- (Exam Topic 3)

Which of the following should be an element of the risk appetite of an organization?

- A. The effectiveness of compensating controls
- B. The enterprise's capacity to absorb loss
- C. The residual risk affected by preventive controls
- D. The amount of inherent risk considered appropriate

Answer: B

NEW QUESTION 102

- (Exam Topic 3)

Several network user accounts were recently created without the required management approvals. Which of the following would be the risk practitioner's BEST recommendation to address this situation?

- A. Conduct a comprehensive compliance review.
- B. Develop incident response procedures for noncompliance.
- C. Investigate the root cause of noncompliance.
- D. Declare a security breach and Inform management.

Answer: C

NEW QUESTION 107

- (Exam Topic 3)

A service provider is managing a client's servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider's MOST appropriate action would be to:

- A. develop a risk remediation plan overriding the client's decision
- B. make a note for this item in the next audit explaining the situation
- C. insist that the remediation occur for the benefit of other customers
- D. ask the client to document the formal risk acceptance for the provider

Answer: D

NEW QUESTION 111

- (Exam Topic 3)

Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

- A. A record of incidents is maintained.
- B. Forensic investigations are facilitated.
- C. Security violations can be identified.
- D. Developing threats are detected earlier.

Answer: C

NEW QUESTION 112

- (Exam Topic 3)

An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

- A. identify key risk indicators (KRIs) for ongoing monitoring
- B. validate the CTO's decision with the business process owner
- C. update the risk register with the selected risk response
- D. recommend that the CTO revisit the risk acceptance decision.

Answer: A

NEW QUESTION 114

- (Exam Topic 3)

An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?

- A. Risk manager
- B. Data owner
- C. End user
- D. IT department

Answer: D

NEW QUESTION 119

- (Exam Topic 3)

While evaluating control costs, management discovers that the annual cost exceeds the annual loss expectancy (ALE) of the risk. This indicates the:

- A. control is ineffective and should be strengthened
- B. risk is inefficiently controlled.
- C. risk is efficiently controlled.
- D. control is weak and should be removed.

Answer: B

NEW QUESTION 124

- (Exam Topic 3)

Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

- A. Automated access revocation
- B. Daily transaction reconciliation
- C. Rule-based data analytics
- D. Role-based user access model

Answer: B

NEW QUESTION 126

- (Exam Topic 3)

An IT department originally planned to outsource the hosting of its data center at an overseas location to reduce operational expenses. After a risk assessment, the department has decided to keep the data center in-house. How should the risk treatment response be reflected in the risk register?

- A. Risk mitigation
- B. Risk avoidance
- C. Risk acceptance
- D. Risk transfer

Answer: A

NEW QUESTION 129

- (Exam Topic 3)

Which of the following is MOST helpful in aligning IT risk with business objectives?

- A. Introducing an approved IT governance framework
- B. Integrating the results of top-down risk scenario analyses
- C. Performing a business impact analysis (BIA)
- D. Implementing a risk classification system

Answer: C

NEW QUESTION 131

- (Exam Topic 3)

Determining if organizational risk is tolerable requires:

- A. mapping residual risk with cost of controls
- B. comparing against regulatory requirements
- C. comparing industry risk appetite with the organization's.
- D. understanding the organization's risk appetite.

Answer: D

NEW QUESTION 133

- (Exam Topic 3)

Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?

- A. KPIs measure manual controls, while KCIs measure automated controls.
- B. KPIs and KCIs both contribute to understanding of control effectiveness.
- C. A robust KCI program will replace the need to measure KPIs.
- D. KCIs are applied at the operational level while KPIs are at the strategic level.

Answer: B

NEW QUESTION 137

- (Exam Topic 3)

While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BEST reduce the risk associated with such a data breach?

- A. Ensuring the vendor does not know the encryption key
- B. Engaging a third party to validate operational controls
- C. Using the same cloud vendor as a competitor
- D. Using field-level encryption with a vendor supplied key

Answer: B

NEW QUESTION 140

- (Exam Topic 3)

When of the following is the MOST significant exposure when an application uses individual user accounts to access the underlying database?

- A. Users may share accounts with business system analyst
- B. Application may not capture a complete audit trail.
- C. Users may be able to circumvent application controls.
- D. Multiple connects to the database are used and slow the process

Answer: C

NEW QUESTION 145

- (Exam Topic 3)

Which of the following is the BEST evidence that a user account has been properly authorized?

- A. An email from the user accepting the account
- B. Notification from human resources that the account is active
- C. User privileges matching the request form
- D. Formal approval of the account by the user's manager

Answer: C

NEW QUESTION 150

- (Exam Topic 3)

Which of the following should be the risk practitioner's FIRST course of action when an organization plans to adopt a cloud computing strategy?

- A. Request a budget for implementation
- B. Conduct a threat analysis.
- C. Create a cloud computing policy.
- D. Perform a controls assessment.

Answer: B

NEW QUESTION 152

- (Exam Topic 3)

An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?

- A. Number of training sessions completed
- B. Percentage of staff members who complete the training with a passing score
- C. Percentage of attendees versus total staff
- D. Percentage of staff members who attend the training with positive feedback

Answer: B

NEW QUESTION 154

- (Exam Topic 3)

Which of the following BEST indicates whether security awareness training is effective?

- A. User self-assessment
- B. User behavior after training
- C. Course evaluation
- D. Quality of training materials

Answer: B

NEW QUESTION 156

- (Exam Topic 3)

Which of the following should be management's PRIMARY focus when key risk indicators (KRIs) begin to rapidly approach defined thresholds?

- A. Designing compensating controls
- B. Determining if KRIs have been updated recently
- C. Assessing the effectiveness of the incident response plan
- D. Determining what has changed in the environment

Answer: D

NEW QUESTION 157

- (Exam Topic 3)

Which of the following should be included in a risk scenario to be used for risk analysis?

- A. Risk appetite
- B. Threat type
- C. Risk tolerance
- D. Residual risk

Answer: B

NEW QUESTION 161

- (Exam Topic 3)

Which of the following BEST indicates how well a web infrastructure protects critical information from an attacker?

- A. Failed login attempts
- B. Simulating a denial of service attack
- C. Absence of IT audit findings
- D. Penetration test

Answer: D

NEW QUESTION 166

- (Exam Topic 3)

Which of the following is the BEST key control indicator (KCI) for risk related to IT infrastructure failure?

- A. Number of times the recovery plan is reviewed
- B. Number of successful recovery plan tests
- C. Percentage of systems with outdated virus protection
- D. Percentage of employees who can work remotely

Answer: B

NEW QUESTION 169

- (Exam Topic 3)

Which of the following would BEST help an enterprise define and communicate its risk appetite?

- A. Gap analysis
- B. Risk assessment
- C. Heat map
- D. Risk register

Answer: C

NEW QUESTION 171

- (Exam Topic 3)

Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information to a supplier?

- A. Encrypt the data while in transit to the supplier
- B. Contractually obligate the supplier to follow privacy laws.
- C. Require independent audits of the supplier's control environment
- D. Utilize blockchain during the data transfer

Answer: B

NEW QUESTION 176

- (Exam Topic 3)

The PRIMARY reason to have risk owners assigned to entries in the risk register is to ensure:

- A. risk is treated appropriately
- B. mitigating actions are prioritized
- C. risk entries are regularly updated
- D. risk exposure is minimized.

Answer: A

NEW QUESTION 177

- (Exam Topic 3)

The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:

- A. inconsistencies between security policies and procedures
- B. possible noncompliant activities that lead to data disclosure
- C. leading or lagging key risk indicators (KRIs)
- D. unknown threats to undermine existing access controls

Answer: B

NEW QUESTION 182

- (Exam Topic 3)

Which of the following is the MOST important objective of an enterprise risk management (ERM) program?

- A. To create a complete repository of risk to the organization
- B. To create a comprehensive view of critical risk to the organization
- C. To provide a bottom-up view of the most significant risk scenarios

D. To optimize costs of managing risk scenarios in the organization

Answer: B

NEW QUESTION 183

- (Exam Topic 3)

Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

- A. Align business objectives with risk appetite.
- B. Enable risk-based decision making.
- C. Design and implement risk response action plans.
- D. Update risk responses in the risk register

Answer: B

NEW QUESTION 185

- (Exam Topic 3)

Which of The following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?

- A. Perform a post-implementation review.
- B. Conduct user acceptance testing.
- C. Review the key performance indicators (KPIs).
- D. Interview process owners.

Answer: C

NEW QUESTION 187

- (Exam Topic 3)

Which of the following is the MOST critical element to maximize the potential for a successful security implementation?

- A. The organization's knowledge
- B. Ease of implementation
- C. The organization's culture
- D. industry-leading security tools

Answer: C

NEW QUESTION 192

- (Exam Topic 3)

Which of the following is the BEST Key control indicator KCO to monitor the effectiveness of patch management?

- A. Percentage of legacy servers out of support
- B. Percentage of servers receiving automata patches
- C. Number of unremediated vulnerabilities
- D. Number of intrusion attempts

Answer: D

NEW QUESTION 197

- (Exam Topic 3)

When of the following 15 MOST important when developing a business case for a proposed security investment?

- A. identification of control requirements
- B. Alignment to business objectives
- C. Consideration of new business strategies
- D. inclusion of strategy for regulatory compliance

Answer: B

NEW QUESTION 198

- (Exam Topic 3)

Which of the following would present the MOST significant risk to an organization when updating the incident response plan?

- A. Obsolete response documentation
- B. Increased stakeholder turnover
- C. Failure to audit third-party providers
- D. Undefined assignment of responsibility

Answer: D

NEW QUESTION 200

- (Exam Topic 3)

An organization is conducting a review of emerging risk. Which of the following is the BEST input for this exercise?

- A. Audit reports

- B. Industry benchmarks
- C. Financial forecasts
- D. Annual threat reports

Answer: B

NEW QUESTION 204

- (Exam Topic 3)

Which of the following is the BEST way to mitigate the risk to IT infrastructure availability?

- A. Establishing a disaster recovery plan (DRP)
- B. Establishing recovery time objectives (RTOs)
- C. Maintaining a current list of staff contact delays
- D. Maintaining a risk register

Answer: D

NEW QUESTION 205

- (Exam Topic 3)

Which of the following is the BEST control to detect an advanced persistent threat (APT)?

- A. Utilizing antivirus systems and firewalls
- B. Conducting regular penetration tests
- C. Monitoring social media activities
- D. Implementing automated log monitoring

Answer: D

NEW QUESTION 209

- (Exam Topic 3)

A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?

- A. Third-party software is used for data analytics.
- B. Data usage exceeds individual consent.
- C. Revenue generated is not disclosed to customers.
- D. Use of a data analytics system is not disclosed to customers.

Answer: B

NEW QUESTION 214

- (Exam Topic 3)

Which of the following is the MOST important consideration for protecting data assets in a Business application system?

- A. Application controls are aligned with data classification rules
- B. Application users are periodically trained on proper data handling practices
- C. Encrypted communication is established between applications and data servers
- D. Offsite encrypted backups are automatically created by the application

Answer: A

NEW QUESTION 217

- (Exam Topic 3)

Which of the following is the BEST evidence of an effective risk treatment plan?

- A. The inherent risk is below the asset residual risk.
- B. Remediation cost is below the asset business value
- C. The risk tolerance threshold is above the asset residual
- D. Remediation is completed within the asset recovery time objective (RTO)

Answer: B

NEW QUESTION 219

- (Exam Topic 3)

An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?

- A. Migrate all data to another compliant service provider.
- B. Analyze the impact of the provider's control weaknesses to the business.
- C. Conduct a follow-up audit to verify the provider's control weaknesses.
- D. Review the contract to determine if penalties should be levied against the provider.

Answer: B

NEW QUESTION 224

- (Exam Topic 3)

When evaluating enterprise IT risk management it is MOST important to:

- A. create new control processes to reduce identified IT risk scenarios
- B. confirm the organization's risk appetite and tolerance
- C. report identified IT risk scenarios to senior management
- D. review alignment with the organization's investment plan

Answer: B

NEW QUESTION 229

- (Exam Topic 3)

Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

- A. Key risk indicators (KRIs)
- B. Risk scenarios
- C. Business impact analysis (BIA)
- D. Threat analysis

Answer: B

NEW QUESTION 231

- (Exam Topic 3)

Which of the following is the GREATEST risk associated with the misclassification of data?

- A. inadequate resource allocation
- B. Data disruption
- C. Unauthorized access
- D. Inadequate retention schedules

Answer: A

NEW QUESTION 232

- (Exam Topic 3)

Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures)?

- A. Mean time to recover (MTTR)
- B. IT system criticality classification
- C. Incident management service level agreement (SLA)
- D. Recovery time objective (RTO)

Answer: D

NEW QUESTION 234

- (Exam Topic 3)

Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

- A. Enable data wipe capabilities
- B. Penetration testing and session timeouts
- C. Implement remote monitoring
- D. Enforce strong passwords and data encryption

Answer: D

NEW QUESTION 236

- (Exam Topic 3)

What are the MOST essential attributes of an effective Key control indicator (KCI)?

- A. Flexibility and adaptability
- B. Measurability and consistency
- C. Robustness and resilience
- D. Optimal cost and benefit

Answer: B

NEW QUESTION 238

- (Exam Topic 3)

In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

- A. Establishing an intellectual property agreement
- B. Evaluating each of the data sources for vulnerabilities
- C. Periodically reviewing big data strategies
- D. Benchmarking to industry best practice

Answer: B

NEW QUESTION 239

- (Exam Topic 3)

When updating the risk register after a risk assessment, which of the following is MOST important to include?

- A. Historical losses due to past risk events
- B. Cost to reduce the impact and likelihood
- C. Likelihood and impact of the risk scenario
- D. Actor and threat type of the risk scenario

Answer: C

NEW QUESTION 242

- (Exam Topic 3)

A risk practitioner is developing a set of bottom-up IT risk scenarios. The MOST important time to involve business stakeholders is when:

- A. updating the risk register
- B. documenting the risk scenarios.
- C. validating the risk scenarios
- D. identifying risk mitigation controls.

Answer: C

NEW QUESTION 245

- (Exam Topic 3)

Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

- A. Poor access control
- B. Unnecessary data storage usage
- C. Data inconsistency
- D. Unnecessary costs of program changes

Answer: C

NEW QUESTION 250

- (Exam Topic 3)

An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

- A. Sufficient resources are not assigned to IT development projects.
- B. Customer support help desk staff does not have adequate training.
- C. Email infrastructure does not have proper rollback plans.
- D. The corporate email system does not identify and store phishing emails.

Answer: A

NEW QUESTION 253

- (Exam Topic 3)

What should be the PRIMARY driver for periodically reviewing and adjusting key risk indicators (KRIs)?

- A. Risk impact
- B. Risk likelihood
- C. Risk appropriate
- D. Control self-assessments (CSAs)

Answer: B

NEW QUESTION 256

- (Exam Topic 3)

Analyzing trends in key control indicators (KCIs) BEST enables a risk practitioner to proactively identify impacts on an organization's:

- A. risk classification methods
- B. risk-based capital allocation
- C. risk portfolio
- D. risk culture

Answer: C

NEW QUESTION 258

- (Exam Topic 3)

Which of the following BEST facilitates the alignment of IT risk management with enterprise risk management (ERM)?

- A. Adopting qualitative enterprise risk assessment methods
- B. Linking IT risk scenarios to technology objectives
- C. linking IT risk scenarios to enterprise strategy
- D. Adopting quantitative enterprise risk assessment methods

Answer:

C

NEW QUESTION 261

- (Exam Topic 3)

Which of the following should be the PRIMARY focus of an IT risk awareness program?

- A. Ensure compliance with the organization's internal policies
- B. Cultivate long-term behavioral change.
- C. Communicate IT risk policy to the participants.
- D. Demonstrate regulatory compliance.

Answer: B

NEW QUESTION 263

- (Exam Topic 3)

Which of the following should be a risk practitioner's PRIMARY focus when tasked with ensuring organization records are being retained for a sufficient period of time to meet legal obligations?

- A. Data duplication processes
- B. Data archival processes
- C. Data anonymization processes
- D. Data protection processes

Answer: B

NEW QUESTION 264

- (Exam Topic 3)

Which of the following methods is an example of risk mitigation?

- A. Not providing capability for employees to work remotely
- B. Outsourcing the IT activities and infrastructure
- C. Enforcing change and configuration management processes
- D. Taking out insurance coverage for IT-related incidents

Answer: C

NEW QUESTION 265

- (Exam Topic 3)

Which of the following is the GREATEST advantage of implementing a risk management program?

- A. Enabling risk-aware decisions
- B. Promoting a risk-aware culture
- C. Improving security governance
- D. Reducing residual risk

Answer: A

NEW QUESTION 267

- (Exam Topic 3)

An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:

- A. reduce the likelihood of future events
- B. restore availability
- C. reduce the impact of future events
- D. address the root cause

Answer: D

NEW QUESTION 271

- (Exam Topic 3)

Which of the following is the BEST source for identifying key control indicators (KCIs)?

- A. Privileged user activity monitoring controls
- B. Controls mapped to organizational risk scenarios
- C. Recent audit findings of control weaknesses
- D. A list of critical security processes

Answer: B

NEW QUESTION 273

- (Exam Topic 3)

An organization learns of a new ransomware attack affecting organizations worldwide. Which of the following should be done FIRST to reduce the likelihood of infection from the attack?

- A. Identify systems that are vulnerable to being exploited by the attack.

- B. Confirm with the antivirus solution vendor whether the next update will detect the attack.
- C. Verify the data backup process and confirm which backups are the most recent ones available.
- D. Obtain approval for funding to purchase a cyber insurance plan.

Answer: A

NEW QUESTION 275

- (Exam Topic 3)

Which of the following BEST enforces access control for an organization that uses multiple cloud technologies?

- A. Senior management support of cloud adoption strategies
- B. Creation of a cloud access risk management policy
- C. Adoption of a cloud access security broker (CASB) solution
- D. Expansion of security information and event management (SIEM) to cloud services

Answer: C

NEW QUESTION 280

- (Exam Topic 3)

A highly regulated organization acquired a medical technology startup company that processes sensitive personal information with weak data protection controls. Which of the following is the BEST way for the acquiring company to reduce its risk while still enabling the flexibility needed by the startup company?

- A. Identify previous data breaches using the startup company's audit reports.
- B. Have the data privacy officer review the startup company's data protection policies.
- C. Classify and protect the data according to the parent company's internal standards.
- D. Implement a firewall and isolate the environment from the parent company's network.

Answer: A

NEW QUESTION 285

- (Exam Topic 3)

Which of The following should be the FIRST step when a company is made aware of new regulatory requirements impacting IT?

- A. Perform a gap analysis.
- B. Prioritize impact to the business units.
- C. Perform a risk assessment.
- D. Review the risk tolerance and appetite.

Answer: C

NEW QUESTION 287

- (Exam Topic 3)

Which of the following controls BEST helps to ensure that transaction data reaches its destination?

- A. Securing the network from attacks
- B. Providing acknowledgments from receiver to sender
- C. Digitally signing individual messages
- D. Encrypting data-in-transit

Answer: B

NEW QUESTION 292

- (Exam Topic 3)

All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

- A. select a provider to standardize the disaster recovery plans.
- B. outsource disaster recovery to an external provider.
- C. centralize the risk response function at the enterprise level.
- D. evaluate opportunities to combine disaster recovery plans.

Answer: D

NEW QUESTION 294

- (Exam Topic 3)

An organization is implementing internet of Things (IoT) technology to control temperature and lighting in its headquarters. Which of the following should be of GREATEST concern?

- A. Insufficient network isolation
- B. impact on network performance
- C. insecure data transmission protocols
- D. Lack of interoperability between sensors

Answer: D

NEW QUESTION 296

- (Exam Topic 4)

The objective of aligning mitigating controls to risk appetite is to ensure that:

- A. exposures are reduced to the fullest extent
- B. exposures are reduced only for critical business systems
- C. insurance costs are minimized
- D. the cost of controls does not exceed the expected loss.

Answer: D

NEW QUESTION 300

- (Exam Topic 4)

Which of the following situations presents the GREATEST challenge to creating a comprehensive IT risk profile of an organization?

- A. Manual vulnerability scanning processes
- B. Organizational reliance on third-party service providers
- C. Inaccurate documentation of enterprise architecture (EA)
- D. Risk-averse organizational risk appetite

Answer: D

NEW QUESTION 302

- (Exam Topic 4)

Recovery the objectives (RTOs) should be based on

- A. minimum tolerable downtime
- B. minimum tolerable loss of data.
- C. maximum tolerable downtime.
- D. maximum tolerable loss of data

Answer: C

NEW QUESTION 303

- (Exam Topic 4)

Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud environment?

- A. Reviewing the results of independent audits
- B. Performing a site visit to the cloud provider's data center
- C. Performing a due diligence review
- D. Conducting a risk workshop with key stakeholders

Answer: D

NEW QUESTION 308

- (Exam Topic 4)

Which of the following is MOST helpful to understand the consequences of an IT risk event?

- A. Fault tree analysis
- B. Historical trend analysis
- C. Root cause analysis
- D. Business impact analysis (BIA)

Answer: B

NEW QUESTION 310

- (Exam Topic 4)

A risk practitioner recently discovered that personal information from the production environment is required for testing purposes in non-production environments. Which of the following is the BEST recommendation to address this situation?

- A. Enable data encryption in the test environment.
- B. Prevent the use of production data in the test environment
- C. De-identify data before being transferred to the test environment.
- D. Enforce multi-factor authentication within the test environment.

Answer: C

NEW QUESTION 313

- (Exam Topic 4)

Which of the following is the BEST way to ensure adequate resources will be allocated to manage identified risk?

- A. Prioritizing risk within each business unit
- B. Reviewing risk ranking methodology
- C. Promoting an organizational culture of risk awareness
- D. Assigning risk ownership to appropriate roles

Answer: D

NEW QUESTION 317

- (Exam Topic 4)

An organization has completed a risk assessment of one of its service providers. Who should be accountable for ensuring that risk responses are implemented?

- A. IT risk practitioner
- B. Third-party security team
- C. The relationship owner
- D. Legal representation of the business

Answer: C

NEW QUESTION 318

- (Exam Topic 4)

Which of the following is the BEST approach to mitigate the risk associated with a control deficiency?

- A. Perform a business case analysis
- B. Implement compensating controls.
- C. Conduct a control self-assessment (CSA)
- D. Build a provision for risk

Answer: C

NEW QUESTION 322

- (Exam Topic 4)

Which of the following will BEST help to ensure new IT policies address the enterprise's requirements?

- A. Involve IT leadership in the policy development process
- B. Require business users to sign acknowledgment of the policies
- C. Involve business owners in the policy development process
- D. Provide policy owners with greater enforcement authority

Answer: B

NEW QUESTION 326

- (Exam Topic 4)

Which of the following sources is MOST relevant to reference when updating security awareness training materials?

- A. Risk management framework
- B. Risk register
- C. Global security standards
- D. Recent security incidents reported by competitors

Answer: B

NEW QUESTION 330

- (Exam Topic 4)

Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

- A. Ensuring processes are documented to enable effective control execution
- B. Ensuring regular risk messaging is included in business communications from leadership
- C. Ensuring schedules and deadlines for control-related deliverables are strictly monitored
- D. Ensuring performance metrics balance business goals with risk appetite

Answer: B

NEW QUESTION 331

- (Exam Topic 4)

Which of the following provides the MOST comprehensive information when developing a risk profile for a system?

- A. Results of a business impact analysis (BIA)
- B. Risk assessment results
- C. A mapping of resources to business processes
- D. Key performance indicators (KPIs)

Answer: B

NEW QUESTION 336

- (Exam Topic 4)

Which of the following standard operating procedure (SOP) statements BEST illustrates appropriate risk register maintenance?

- A. Remove risk that has been mitigated by third-party transfer
- B. Remove risk that management has decided to accept
- C. Remove risk only following a significant change in the risk environment

D. Remove risk when mitigation results in residual risk within tolerance levels

Answer: C

NEW QUESTION 337

- (Exam Topic 4)

Business management is seeking assurance from the CIO that IT has a plan in place for early identification of potential issues that could impact the delivery of a new application. Which of the following is the BEST way to increase the chances of a successful delivery'?

- A. Implement a release and deployment plan
- B. Conduct comprehensive regression testing.
- C. Develop enterprise-wide key risk indicators (KRIs)
- D. Include business management on a weekly risk and issues report

Answer: D

NEW QUESTION 342

- (Exam Topic 4)

When implementing an IT risk management program, which of the following is the BEST time to evaluate current control effectiveness?

- A. Before defining a framework
- B. During the risk assessment
- C. When evaluating risk response
- D. When updating the risk register

Answer: B

NEW QUESTION 345

- (Exam Topic 4)

Which of the following is the PRIMARY reason for sharing risk assessment reports with senior stakeholders?

- A. To support decision-making for risk response
- B. To hold risk owners accountable for risk action plans
- C. To secure resourcing for risk treatment efforts
- D. To enable senior management to compile a risk profile

Answer: A

NEW QUESTION 347

- (Exam Topic 4)

Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

- A. Verifying that project objectives are met
- B. Identifying project cost overruns
- C. Leveraging an independent review team
- D. Reviewing the project initiation risk matrix

Answer: A

NEW QUESTION 351

- (Exam Topic 4)

During an acquisition, which of the following would provide the MOST useful input to the parent company's risk practitioner when developing risk scenarios for the post-acquisition phase?

- A. Risk management framework adopted by each company
- B. Risk registers of both companies
- C. IT balanced scorecard of each company
- D. Most recent internal audit findings from both companies

Answer: C

NEW QUESTION 352

- (Exam Topic 4)

The PRIMARY objective of collecting information and reviewing documentation when performing periodic risk analysis should be to:

- A. Identify new or emerging risk issues.
- B. Satisfy audit requirements.
- C. Survey and analyze historical risk data.
- D. Understand internal and external threat agents.

Answer: D

NEW QUESTION 354

- (Exam Topic 4)

Following an acquisition, the acquiring company's risk practitioner has been asked to update the organization's IT risk profile. What is the MOST important

information to review from the acquired company to facilitate this task?

- A. Internal and external audit reports
- B. Risk disclosures in financial statements
- C. Risk assessment and risk register
- D. Business objectives and strategies

Answer: C

NEW QUESTION 357

- (Exam Topic 4)

Which of the following BEST enables effective IT control implementation?

- A. Key risk indicators (KRIs)
- B. Documented procedures
- C. Information security policies
- D. Information security standards

Answer: B

NEW QUESTION 359

- (Exam Topic 4)

A zero-day vulnerability has been discovered in a globally used brand of hardware server that allows hackers to gain access to affected IT systems. Which of the following is MOST likely to change as a result of this situation?

- A. Control effectiveness
- B. Risk appetite
- C. Risk likelihood
- D. Key risk indicator (KRI)

Answer: C

NEW QUESTION 361

- (Exam Topic 4)

Which of the following is the MOST important reason to validate that risk responses have been executed as outlined in the risk response plan?"

- A. To ensure completion of the risk assessment cycle
- B. To ensure controls are operating effectively
- C. To ensure residual risk is at an acceptable level
- D. To ensure control costs do not exceed benefits

Answer: A

NEW QUESTION 365

- (Exam Topic 4)

When preparing a risk status report for periodic review by senior management, it is MOST important to ensure the report includes

- A. risk exposure in business terms
- B. a detailed view of individual risk exposures
- C. a summary of incidents that have impacted the organization.
- D. recommendations by an independent risk assessor.

Answer: A

NEW QUESTION 367

- (Exam Topic 4)

The BEST indicator of the risk appetite of an organization is the

- A. regulatory environment of the organization
- B. risk management capability of the organization
- C. board of directors' response to identified risk factors
- D. importance assigned to IT in meeting strategic goals

Answer: B

NEW QUESTION 371

- (Exam Topic 4)

Which of the following would MOST likely require a risk practitioner to update the risk register?

- A. An alert being reported by the security operations center.
- B. Development of a project schedule for implementing a risk response
- C. Completion of a project for implementing a new control
- D. Engagement of a third party to conduct a vulnerability scan

Answer: C

NEW QUESTION 376

- (Exam Topic 4)

An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

- A. The volume of risk scenarios is too large
- B. Risk aggregation has not been completed
- C. Risk scenarios are not applicable
- D. The risk analysts for each scenario is incomplete

Answer: D

NEW QUESTION 377

- (Exam Topic 4)

An organization wants to grant remote access to a system containing sensitive data to an overseas third party. Which of the following should be of GREATEST concern to management?

- A. Transborder data transfer restrictions
- B. Differences in regional standards
- C. Lack of monitoring over vendor activities
- D. Lack of after-hours incident management support

Answer: C

NEW QUESTION 381

- (Exam Topic 4)

Which of the following should be used as the PRIMARY basis for evaluating the state of an organization's cloud computing environment against leading practices?

- A. The cloud environment's capability maturity model
- B. The cloud environment's risk register
- C. The cloud computing architecture
- D. The organization's strategic plans for cloud computing

Answer: A

NEW QUESTION 383

- (Exam Topic 4)

An organization has operations in a location that regularly experiences severe weather events. Which of the following would BEST help to mitigate the risk to operations?

- A. Prepare a cost-benefit analysis to evaluate relocation.
- B. Prepare a disaster recovery plan (DRP).
- C. Conduct a business impact analysis (BIA) for an alternate location.
- D. Develop a business continuity plan (BCP).

Answer: D

NEW QUESTION 387

- (Exam Topic 4)

One of an organization's key IT systems cannot be patched because the patches interfere with critical business application functionalities. Which of the following would be the risk practitioner's BEST recommendation?

- A. Additional mitigating controls should be identified.
- B. The system should not be used until the application is changed
- C. The organization's IT risk appetite should be adjusted.
- D. The associated IT risk should be accepted by management.

Answer: A

NEW QUESTION 392

- (Exam Topic 4)

Which of the following is the MAIN purpose of monitoring risk?

- A. Communication
- B. Risk analysis
- C. Decision support
- D. Benchmarking

Answer: A

NEW QUESTION 395

- (Exam Topic 4)

To define the risk management strategy which of the following MUST be set by the board of directors?

- A. Operational strategies
- B. Risk governance
- C. Annualized loss expectancy (ALE)

D. Risk appetite

Answer: B

NEW QUESTION 397

- (Exam Topic 4)

Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

- A. Verify authorization by senior management.
- B. Increase the risk appetite to align with the current risk level
- C. Ensure the acceptance is set to expire over time
- D. Update the risk response in the risk register.

Answer: A

NEW QUESTION 398

- (Exam Topic 4)

Which of the following is MOST important when implementing an organization's security policy?

- A. Obtaining management support
- B. Benchmarking against industry standards
- C. Assessing compliance requirements
- D. Identifying threats and vulnerabilities

Answer: A

NEW QUESTION 403

- (Exam Topic 4)

When developing risk scenarios using a list of generic scenarios based on industry best practices, it is MOST important to:

- A. Assess generic risk scenarios with business users.
- B. Validate the generic risk scenarios for relevance.
- C. Select the maximum possible risk scenarios from the list.
- D. Identify common threats causing generic risk scenarios

Answer: B

NEW QUESTION 404

- (Exam Topic 4)

Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

- A. Implement user access controls
- B. Perform regular internal audits
- C. Develop and communicate fraud prevention policies
- D. Conduct fraud prevention awareness training.

Answer: A

NEW QUESTION 405

- (Exam Topic 4)

An organization control environment is MOST effective when:

- A. control designs are reviewed periodically
- B. controls perform as intended.
- C. controls are implemented consistently.
- D. controls operate efficiently

Answer: B

NEW QUESTION 406

- (Exam Topic 4)

Which of the following is the PRIMARY reason to engage business unit managers in risk management processes?

- A. Improved alignment with technical risk
- B. Better-informed business decisions
- C. Enhanced understanding of enterprise architecture (EA)
- D. Improved business operations efficiency

Answer: C

NEW QUESTION 409

- (Exam Topic 4)

When defining thresholds for control key performance indicators (KPIs), it is MOST helpful to align:

- A. information risk assessments with enterprise risk assessments.

- B. key risk indicators (KRIs) with risk appetite of the business.
- C. the control key performance indicators (KPIs) with audit findings.
- D. control performance with risk tolerance of business owners.

Answer: B

NEW QUESTION 411

- (Exam Topic 4)

Which of the following is the MOST important consideration when communicating the risk associated with technology end-of-life to business owners?

- A. Cost and benefit
- B. Security and availability
- C. Maintainability and reliability
- D. Performance and productivity

Answer: A

NEW QUESTION 415

- (Exam Topic 4)

An organization's recovery team is attempting to recover critical data backups following a major flood in its data center. However, key team members do not know exactly what steps should be taken to address this crisis. Which of the following is the MOST likely cause of this situation?

- A. Failure to test the disaster recovery plan (DRP)
- B. Lack of well-documented business impact analysis (BIA)
- C. Lack of annual updates to the disaster recovery plan (DRP)
- D. Significant changes in management personnel

Answer: A

NEW QUESTION 416

- (Exam Topic 4)

Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

- A. KRIs provide an early warning that a risk threshold is about to be reached.
- B. KRIs signal that a change in the control environment has occurred.
- C. KRIs provide a basis to set the risk appetite for an organization.
- D. KRIs assist in the preparation of the organization's risk profile.

Answer: A

NEW QUESTION 421

- (Exam Topic 4)

When reviewing the business continuity plan (BCP) of an online sales order system, a risk practitioner notices that the recovery time objective (RTO) has a shorter time than what is defined in the disaster recovery plan (DRP). Which of the following is the BEST way for the risk practitioner to address this concern?

- A. Adopt the RTO defined in the BCR
- B. Update the risk register to reflect the discrepancy.
- C. Adopt the RTO defined in the DRP.
- D. Communicate the discrepancy to the DR manager for follow-up.

Answer: D

NEW QUESTION 422

- (Exam Topic 4)

An organization has experienced a cyber attack that exposed customer personally identifiable information (PII) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

- A. Security control owners based on control failures
- B. Cyber risk remediation plan owners
- C. Risk owners based on risk impact
- D. Enterprise risk management (ERM) team

Answer: C

NEW QUESTION 426

- (Exam Topic 4)

An organization has experienced several incidents of extended network outages that have exceeded tolerance. Which of the following should be the risk practitioner's FIRST step to address this situation?

- A. Recommend additional controls to address the risk.
- B. Update the risk tolerance level to acceptable thresholds.
- C. Update the incident-related risk trend in the risk register.
- D. Recommend a root cause analysis of the incidents.

Answer: D

NEW QUESTION 431

- (Exam Topic 4)

Which of the following is MOST important to promoting a risk-aware culture?

- A. Regular testing of risk controls
- B. Communication of audit findings
- C. Procedures for security monitoring
- D. Open communication of risk reporting

Answer: D

NEW QUESTION 433

- (Exam Topic 4)

Which of the following BEST helps to identify significant events that could impact an organization?

- A. Control analysis
- B. Vulnerability analysis
- C. Scenario analysis
- D. Heat map analysis

Answer: C

NEW QUESTION 434

- (Exam Topic 4)

Which of the following is the BEST approach for selecting controls to minimize risk?

- A. Industry best practice review
- B. Risk assessment
- C. Cost-benefit analysis
- D. Control-effectiveness evaluation

Answer: C

NEW QUESTION 438

- (Exam Topic 4)

Which of the following is the BEST method of creating risk awareness in an organization?

- A. Marking the risk register available to project stakeholders
- B. Ensuring senior management commitment to risk training
- C. Providing regular communication to risk managers
- D. Appointing the risk manager from the business units

Answer: B

NEW QUESTION 442

- (Exam Topic 4)

Which of the following proposed benefits is MOST likely to influence senior management approval to reallocate budget for a new security initiative?

- A. Reduction in the number of incidents
- B. Reduction in inherent risk
- C. Reduction in residual risk
- D. Reduction in the number of known vulnerabilities

Answer: B

NEW QUESTION 447

- (Exam Topic 4)

Which of the following provides the MOST reliable evidence of a control's effectiveness?

- A. A risk and control self-assessment
- B. Senior management's attestation
- C. A system-generated testing report
- D. detailed process walk-through

Answer: D

NEW QUESTION 448

- (Exam Topic 4)

Which of the following is the PRIMARY objective of establishing an organization's risk tolerance and appetite?

- A. To align with board reporting requirements
- B. To assist management in decision making
- C. To create organization-wide risk awareness
- D. To minimize risk mitigation efforts

Answer: B

NEW QUESTION 451

- (Exam Topic 4)

Which of the following would be the BEST way for a risk practitioner to validate the effectiveness of a patching program?

- A. Conduct penetration testing.
- B. Interview IT operations personnel.
- C. Conduct vulnerability scans.
- D. Review change control board documentation.

Answer: C

NEW QUESTION 454

- (Exam Topic 4)

Effective risk communication BEST benefits an organization by:

- A. helping personnel make better-informed decisions
- B. assisting the development of a risk register.
- C. improving the effectiveness of IT controls.
- D. increasing participation in the risk assessment process.

Answer: A

NEW QUESTION 455

- (Exam Topic 4)

Before assigning sensitivity levels to information it is MOST important to:

- A. define recovery time objectives (RTOs).
- B. define the information classification policy
- C. conduct a sensitivity analyse
- D. Identify information custodians

Answer: B

NEW QUESTION 456

- (Exam Topic 4)

Which of the following is MOST useful for measuring the existing risk management process against a desired state?

- A. Balanced scorecard
- B. Risk management framework
- C. Capability maturity model
- D. Risk scenario analysis

Answer: C

NEW QUESTION 459

- (Exam Topic 4)

Which of the following is the result of a realized risk scenario?

- A. Threat event
- B. Vulnerability event
- C. Technical event
- D. Loss event

Answer: D

NEW QUESTION 462

- (Exam Topic 4)

Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

- A. Internal auditor
- B. Asset owner
- C. Finance manager
- D. Control owner

Answer: B

NEW QUESTION 464

- (Exam Topic 4)

After an annual risk assessment is completed, which of the following would be MOST important to communicate to stakeholders?

- A. A decrease in threats
- B. A change in the risk profile
- C. An increase in reported vulnerabilities
- D. An increase in identified risk scenarios

Answer:

B

NEW QUESTION 468

- (Exam Topic 4)

A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?

- A. Collaborate with the risk owner to determine the risk response plan.
- B. Document the gap in the risk register and report to senior management.
- C. Include a right to audit clause in the service provider contract.
- D. Advise the risk owner to accept the risk.

Answer: A

NEW QUESTION 472

- (Exam Topic 4)

Which of the following is the MOST important step to ensure regulatory requirements are adequately addressed within an organization?

- A. Obtain necessary resources to address regulatory requirements
- B. Develop a policy framework that addresses regulatory requirements
- C. Perform a gap analysis against regulatory requirements.
- D. Employ IT solutions that meet regulatory requirements.

Answer: B

NEW QUESTION 477

- (Exam Topic 4)

Which of the following is the MOST effective way for a large and diversified organization to minimize risk associated with unauthorized software on company devices?

- A. Scan end points for applications not included in the asset inventory.
- B. Prohibit the use of cloud-based virtual desktop software.
- C. Conduct frequent reviews of software licenses.
- D. Perform frequent internal audits of enterprise IT infrastructure.

Answer: A

NEW QUESTION 482

- (Exam Topic 4)

Which of the following is the MOST useful information for a risk practitioner when planning response activities after risk identification?

- A. Risk register
- B. Risk appetite
- C. Risk priorities
- D. Risk heat maps

Answer: B

NEW QUESTION 483

- (Exam Topic 4)

An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:

- A. a recognized industry control framework
- B. guidance provided by the external auditor
- C. the service provider's existing controls
- D. The organization's specific control requirements

Answer: D

NEW QUESTION 485

- (Exam Topic 4)

An organization is implementing robotic process automation (RPA) to streamline business processes. Given that implementation of this technology is expected to impact existing controls, which of the following is the risk practitioner's BEST course of action?

- A. Reassess whether mitigating controls address the known risk in the processes.
- B. Update processes to address the new technology.
- C. Update the data governance policy to address the new technology.
- D. Perform a gap analysis of the impacted processes.

Answer: A

NEW QUESTION 489

- (Exam Topic 4)

Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

- A. Some critical business applications are not included in the plan
- B. Several recovery activities will be outsourced
- C. The plan is not based on an internationally recognized framework
- D. The chief information security officer (CISO) has not approved the plan

Answer: A

NEW QUESTION 490

- (Exam Topic 4)

A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

- A. Risk manager
- B. Control owner
- C. Control tester
- D. Risk owner

Answer: B

NEW QUESTION 491

- (Exam Topic 4)

Which of the following should be the PRIMARY input to determine risk tolerance?

- A. Regulatory requirements
- B. Organizational objectives
- C. Annual loss expectancy (ALE)
- D. Risk management costs

Answer: C

NEW QUESTION 495

- (Exam Topic 4)

After entering a large number of low-risk scenarios into the risk register, it is MOST important for the risk practitioner to:

- A. prepare a follow-up risk assessment.
- B. recommend acceptance of the risk scenarios.
- C. reconfirm risk tolerance levels.
- D. analyze changes to aggregate risk.

Answer: D

NEW QUESTION 498

- (Exam Topic 4)

The BEST key performance indicator (KPI) to measure the effectiveness of the security patching process is the percentage of patches installed:

- A. by the security administration team.
- B. successfully within the expected time frame.
- C. successfully during the first attempt.
- D. without causing an unplanned system outage.

Answer: B

NEW QUESTION 501

- (Exam Topic 4)

Which of the following will BEST ensure that controls adequately support business goals and objectives?

- A. Using the risk management process
- B. Enforcing strict disciplinary procedures in case of noncompliance
- C. Reviewing results of the annual company external audit
- D. Adopting internationally accepted controls

Answer: A

NEW QUESTION 504

- (Exam Topic 4)

A newly incorporated enterprise needs to secure its information assets From a governance perspective which of the following should be done FIRST?

- A. Define information retention requirements and policies
- B. Provide information security awareness training
- C. Establish security management processes and procedures
- D. Establish an inventory of information assets

Answer: D

NEW QUESTION 506

- (Exam Topic 4)

Which of the following is MOST important for an organization to consider when developing its IT strategy?

- A. IT goals and objectives
- B. Organizational goals and objectives
- C. The organization's risk appetite statement
- D. Legal and regulatory requirements

Answer: C

NEW QUESTION 508

- (Exam Topic 3)

Which of the following would MOST likely cause a risk practitioner to change the likelihood rating in the risk register?

- A. Risk appetite
- B. Control cost
- C. Control effectiveness
- D. Risk tolerance

Answer: C

NEW QUESTION 509

- (Exam Topic 3)

An information system for a key business operation is being moved from an in-house application to a Software as a Service (SaaS) vendor. Which of the following will have the GREATEST impact on the ability to monitor risk?

- A. Reduced ability to evaluate key risk indicators (KRIs)
- B. Reduced access to internal audit reports
- C. Dependency on the vendor's key performance indicators (KPIs)
- D. Dependency on service level agreements (SLAs)

Answer: A

NEW QUESTION 510

- (Exam Topic 3)

Which of the following BEST indicates that additional or improved controls are needed in the environment?

- A. Management has decreased organisational risk appetite
- B. The risk register and portfolio do not include all risk scenarios
- C. Emerging risk scenarios have been identified
- D. Risk events and losses exceed risk tolerance

Answer: D

NEW QUESTION 515

- (Exam Topic 3)

A risk practitioner has been asked by executives to explain how existing risk treatment plans would affect risk posture at the end of the year. Which of the following is MOST helpful in responding to this request?

- A. Assessing risk with no controls in place
- B. Showing projected residual risk
- C. Providing peer benchmarking results
- D. Assessing risk with current controls in place

Answer: D

NEW QUESTION 520

- (Exam Topic 3)

An organization's risk register contains a large volume of risk scenarios that senior management considers overwhelming. Which of the following would BEST help to improve the risk register?

- A. Analyzing the residual risk components
- B. Performing risk prioritization
- C. Validating the risk appetite level
- D. Conducting a risk assessment

Answer: D

NEW QUESTION 522

- (Exam Topic 3)

Which of the following is the STRONGEST indication an organization has ethics management issues?

- A. Employees do not report IT risk issues for fear of consequences.
- B. Internal IT auditors report to the chief information security officer (CISO).
- C. Employees face sanctions for not signing the organization's acceptable use policy.
- D. The organization has only two lines of defense.

Answer: A

NEW QUESTION 524

- (Exam Topic 3)

Which of the following BEST assists in justifying an investment in automated controls?

- A. Cost-benefit analysis
- B. Alignment of investment with risk appetite
- C. Elimination of compensating controls
- D. Reduction in personnel costs

Answer: A

NEW QUESTION 526

- (Exam Topic 3)

The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

- A. availability of fault tolerant software.
- B. strategic plan for business growth.
- C. vulnerability scan results of critical systems.
- D. redundancy of technical infrastructure.

Answer: D

NEW QUESTION 528

- (Exam Topic 3)

Which of the following is the FIRST step in risk assessment?

- A. Review risk governance
- B. Asset identification
- C. Identify risk factors
- D. Inherent risk identification

Answer: B

NEW QUESTION 532

- (Exam Topic 3)

An organization's IT infrastructure is running end-of-life software that is not allowed without exception approval. Which of the following would provide the MOST helpful information to justify investing in updated software?

- A. The balanced scorecard
- B. A cost-benefit analysis
- C. The risk management framework
- D. A roadmap of IT strategic planning

Answer: B

NEW QUESTION 534

- (Exam Topic 3)

A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

- A. Monitor processes to ensure recent updates are being followed.
- B. Communicate to those who test and promote changes.
- C. Conduct a cost-benefit analysis to justify the cost of the control.
- D. Assess the maturity of the change management process.

Answer: A

NEW QUESTION 539

- (Exam Topic 3)

What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

- A. Ensure compliance.
- B. Identify trends.
- C. Promote a risk-aware culture.
- D. Optimize resources needed for controls

Answer: A

NEW QUESTION 543

- (Exam Topic 3)

The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

- A. resources to monitor backups
- B. restoration monitoring reports
- C. backup recovery requests

D. recurring restore failures

Answer: D

NEW QUESTION 544

- (Exam Topic 3)

The BEST reason to classify IT assets during a risk assessment is to determine the:

- A. priority in the risk register.
- B. business process owner.
- C. enterprise risk profile.
- D. appropriate level of protection.

Answer: D

NEW QUESTION 545

- (Exam Topic 3)

An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?

- A. Conduct a risk analysis.
- B. Initiate a remote data wipe.
- C. Invoke the incident response plan
- D. Disable the user account.

Answer: C

NEW QUESTION 550

- (Exam Topic 3)

Which of the following poses the GREATEST risk to an organization's operations during a major it transformation?

- A. Lack of robust awareness programs
- B. infrequent risk assessments of key controls
- C. Rapid changes in IT procedures
- D. Unavailability of critical IT systems

Answer: D

NEW QUESTION 553

- (Exam Topic 3)

The BEST indication that risk management is effective is when risk has been reduced to meet:

- A. risk levels.
- B. risk budgets.
- C. risk appetite.
- D. risk capacity.

Answer: C

NEW QUESTION 554

- (Exam Topic 3)

Which of the following is the BEST way to assess the effectiveness of an access management process?

- A. Comparing the actual process with the documented process
- B. Reviewing access logs for user activity
- C. Reconciling a list of accounts belonging to terminated employees
- D. Reviewing for compliance with acceptable use policy

Answer: B

NEW QUESTION 555

- (Exam Topic 3)

Which of the following BEST mitigates the risk of sensitive personal data leakage from a software development environment?

- A. Tokenized personal data only in test environments
- B. Data loss prevention tools (DLP) installed in passive mode
- C. Anonymized personal data in non-production environments
- D. Multi-factor authentication for access to non-production environments

Answer: C

NEW QUESTION 557

- (Exam Topic 3)

Which of the following BEST indicates the efficiency of a process for granting access privileges?

- A. Average time to grant access privileges

- B. Number of changes in access granted to users
- C. Average number of access privilege exceptions
- D. Number and type of locked obsolete accounts

Answer: C

NEW QUESTION 562

- (Exam Topic 3)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery test of critical business processes?

- A. Percentage of job failures identified and resolved during the recovery process
- B. Percentage of processes recovered within the recovery time and point objectives
- C. Number of current test plans and procedures
- D. Number of issues and action items resolved during the recovery test

Answer: B

NEW QUESTION 565

- (Exam Topic 3)

Which of the following is a drawback in the use of quantitative risk analysis?

- A. It assigns numeric values to exposures of assets.
- B. It requires more resources than other methods
- C. It produces the results in numeric form.
- D. It is based on impact analysis of information assets.

Answer: B

NEW QUESTION 566

- (Exam Topic 3)

A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

- A. Monitor the databases for abnormal activity
- B. Approve exception to allow the software to continue operating
- C. Require the software vendor to remediate the vulnerabilities
- D. Accept the risk and let the vendor run the software as is

Answer: C

NEW QUESTION 567

- (Exam Topic 3)

A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:

- A. management.
- B. tolerance.
- C. culture.
- D. analysis.

Answer: C

NEW QUESTION 570

- (Exam Topic 3)

Which of the following would provide the MOST useful information to a risk owner when reviewing the progress of risk mitigation?

- A. Key audit findings
- B. Treatment plan status
- C. Performance indicators
- D. Risk scenario results

Answer: C

NEW QUESTION 573

- (Exam Topic 3)

Which of the following is the BEST way for an organization to enable risk treatment decisions?

- A. Allocate sufficient funds for risk remediation.
- B. Promote risk and security awareness.
- C. Establish clear accountability for risk.
- D. Develop comprehensive policies and standards.

Answer: C

NEW QUESTION 574

- (Exam Topic 3)

In an organization that allows employee use of social media accounts for work purposes, which of the following is the BEST way to protect company sensitive information from being exposed?

- A. Educating employees on what needs to be kept confidential
- B. Implementing a data loss prevention (DLP) solution
- C. Taking punitive action against employees who expose confidential data
- D. Requiring employees to sign nondisclosure agreements

Answer: B

NEW QUESTION 579

- (Exam Topic 3)

A risk practitioner has become aware of production data being used in a test environment. Which of the following should be the practitioner's PRIMARY concern?

- A. Sensitivity of the data
- B. Readability of test data
- C. Security of the test environment
- D. Availability of data to authorized staff

Answer: A

NEW QUESTION 582

- (Exam Topic 3)

The GREATEST benefit of including low-probability, high-impact events in a risk assessment is the ability to:

- A. develop a comprehensive risk mitigation strategy
- B. develop understandable and realistic risk scenarios
- C. identify root causes for relevant events
- D. perform an aggregated cost-benefit analysis

Answer: D

NEW QUESTION 585

- (Exam Topic 3)

To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:

- A. require the vendor to sign a nondisclosure agreement
- B. clearly define the project scope.
- C. perform background checks on the vendor.
- D. notify network administrators before testing

Answer: A

NEW QUESTION 589

- (Exam Topic 3)

Which of the following would be a risk practitioner's BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

- A. Manage cyber risk according to the organization's risk management framework.
- B. Define cyber roles and responsibilities across the organization
- C. Conduct cyber risk awareness training tailored specifically for senior management
- D. Implement a cyber risk program based on industry best practices

Answer: B

NEW QUESTION 592

- (Exam Topic 3)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an antivirus program?

- A. Percentage of IT assets with current malware definitions
- B. Number of false positives detected over a period of time
- C. Number of alerts generated by the anti-virus software
- D. Frequency of anti-virus software updates

Answer: A

NEW QUESTION 597

- (Exam Topic 3)

Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

- A. Control self-assessment (CSA)
- B. Security information and event management (SIEM) solutions
- C. Data privacy impact assessment (DPIA)
- D. Data loss prevention (DLP) tools

Answer: B

NEW QUESTION 598

- (Exam Topic 3)

Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:

- A. a threat.
- B. a vulnerability.
- C. an impact
- D. a control.

Answer: B

NEW QUESTION 601

- (Exam Topic 3)

An organization practices the principle of least privilege. To ensure access remains appropriate, application owners should be required to review user access rights on a regular basis by obtaining:

- A. business purpose documentation and software license counts
- B. an access control matrix and approval from the user's manager
- C. documentation indicating the intended users of the application
- D. security logs to determine the cause of invalid login attempts

Answer: B

NEW QUESTION 604

- (Exam Topic 3)

The MOST important consideration when selecting a control to mitigate an identified risk is whether:

- A. the cost of control exceeds the mitigation value
- B. there are sufficient internal resources to implement the control
- C. the mitigation measures create compounding effects
- D. the control eliminates the risk

Answer: A

NEW QUESTION 609

- (Exam Topic 3)

Which of the following should be the MOST important consideration when performing a vendor risk assessment?

- A. Results of the last risk assessment of the vendor
- B. Inherent risk of the business process supported by the vendor
- C. Risk tolerance of the vendor
- D. Length of time since the last risk assessment of the vendor

Answer: B

NEW QUESTION 611

- (Exam Topic 3)

Which of the following provides the MOST useful information when developing a risk profile for management approval?

- A. Residual risk and risk appetite
- B. Strength of detective and preventative controls
- C. Effectiveness and efficiency of controls
- D. Inherent risk and risk tolerance

Answer: A

NEW QUESTION 614

- (Exam Topic 3)

An IT risk practitioner has been asked to regularly report on the overall status and effectiveness of the IT risk management program. Which of the following is MOST useful for this purpose?

- A. Balanced scorecard
- B. Capability maturity level
- C. Internal audit plan
- D. Control self-assessment (CSA)

Answer: A

NEW QUESTION 616

- (Exam Topic 3)

While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

- A. review and update the policies to align with industry standards.
- B. determine that the policies should be updated annually.
- C. report that the policies are adequate and do not need to be updated frequently.

D. review the policies against current needs to determine adequacy.

Answer: D

NEW QUESTION 618

- (Exam Topic 3)

Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?

- A. Data encryption has not been applied to all sensitive data across the organization.
- B. There are many data assets across the organization that need to be classified.
- C. Changes to information handling procedures are not documented.
- D. Changes to data sensitivity during the data life cycle have not been considered.

Answer: D

NEW QUESTION 621

- (Exam Topic 3)

Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?

- A. Piloting courses with focus groups
- B. Using reputable third-party training programs
- C. Reviewing content with senior management
- D. Creating modules for targeted audiences

Answer: D

NEW QUESTION 622

- (Exam Topic 2)

Which of the following is the BEST indicator of the effectiveness of a control action plan's implementation?

- A. Increased number of controls
- B. Reduced risk level
- C. Increased risk appetite
- D. Stakeholder commitment

Answer: B

NEW QUESTION 623

- (Exam Topic 2)

A risk practitioner has just learned about new done FIRST?

- A. Notify executive management.
- B. Analyze the impact to the organization.
- C. Update the IT risk register.
- D. Design IT risk mitigation plans.

Answer: B

NEW QUESTION 625

- (Exam Topic 2)

Which of the following is MOST important when defining controls?

- A. Identifying monitoring mechanisms
- B. Including them in the risk register
- C. Aligning them with business objectives
- D. Prototyping compensating controls

Answer: C

NEW QUESTION 628

- (Exam Topic 2)

Which of the following is the MOST important consideration when selecting either a qualitative or quantitative risk analysis?

- A. Expertise in both methodologies
- B. Maturity of the risk management program
- C. Time available for risk analysis
- D. Resources available for data analysis

Answer: D

NEW QUESTION 632

- (Exam Topic 2)

A risk practitioner shares the results of a vulnerability assessment for a critical business application with the business manager. Which of the following is the NEXT step?

- A. Develop a risk action plan to address the findings.
- B. Evaluate the impact of the vulnerabilities to the business application.
- C. Escalate the findings to senior management and internal audit.
- D. Conduct a penetration test to validate the vulnerabilities from the findings.

Answer: B

NEW QUESTION 634

- (Exam Topic 2)

An organization plans to migrate sensitive information to a public cloud infrastructure. Which of the following is the GREATEST security risk in this scenario?

- A. Data may be commingled with other tenants' data.
- B. System downtime does not meet the organization's thresholds.
- C. The infrastructure will be managed by the public cloud administrator.
- D. The cloud provider is not independently certified.

Answer: A

NEW QUESTION 637

- (Exam Topic 2)

When assessing the maturity level of an organization's risk management framework, which of the following deficiencies should be of GREATEST concern to a risk practitioner?

- A. Unclear organizational risk appetite
- B. Lack of senior management participation
- C. Use of highly customized control frameworks
- D. Reliance on qualitative analysis methods

Answer: C

NEW QUESTION 639

- (Exam Topic 2)

Who should be responsible for strategic decisions on risk management?

- A. Chief information officer (CIO)
- B. Executive management team
- C. Audit committee
- D. Business process owner

Answer: B

NEW QUESTION 644

- (Exam Topic 2)

The BEST way to test the operational effectiveness of a data backup procedure is to:

- A. conduct an audit of files stored offsite.
- B. interview employees to compare actual with expected procedures.
- C. inspect a selection of audit trails and backup logs.
- D. demonstrate a successful recovery from backup files.

Answer: D

NEW QUESTION 649

- (Exam Topic 2)

Which of the following statements in an organization's current risk profile report is cause for further action by senior management?

- A. Key performance indicator (KPI) trend data is incomplete.
- B. New key risk indicators (KRIs) have been established.
- C. Key performance indicators (KPIs) are outside of targets.
- D. Key risk indicators (KRIs) are lagging.

Answer: B

NEW QUESTION 652

- (Exam Topic 2)

Which of the following conditions presents the GREATEST risk to an application?

- A. Application controls are manual.
- B. Application development is outsourced.
- C. Source code is escrowed.
- D. Developers have access to production environment.

Answer: D

NEW QUESTION 657

- (Exam Topic 2)

An organization's internal audit department is considering the implementation of robotics process automation (RPA) to automate certain continuous auditing tasks. Who would own the risk associated with ineffective design of the software bots?

- A. Lead auditor
- B. Project manager
- C. Chief audit executive (CAE)
- D. Chief information officer (CIO)

Answer: C

NEW QUESTION 661

- (Exam Topic 2)

What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

- A. Risk and control ownership
- B. Senior management participation
- C. Business unit support
- D. Risk nomenclature and taxonomy

Answer: B

NEW QUESTION 666

- (Exam Topic 2)

Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

- A. Key risk indicators (KRIs)
- B. Data backups
- C. Incident response plan
- D. Cyber insurance

Answer: C

NEW QUESTION 670

- (Exam Topic 2)

An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Alpha	High	Medium	High
Bravo	High	Low	Medium
Charlie	High	High	High
Delta	High	Medium	Medium

- A. Project Charlie
- B. Project Bravo
- C. Project Alpha
- D. Project Delta

Answer: A

NEW QUESTION 671

- (Exam Topic 2)

Deviation from a mitigation action plan's completion date should be determined by which of the following?

- A. Change management as determined by a change control board
- B. Benchmarking analysis with similar completed projects
- C. Project governance criteria as determined by the project office
- D. The risk owner as determined by risk management processes

Answer: D

NEW QUESTION 675

- (Exam Topic 2)

Which of the following is the MOST important information to be communicated during security awareness training?

- A. Management's expectations
- B. Corporate risk profile
- C. Recent security incidents
- D. The current risk management capability

Answer: A

NEW QUESTION 677

- (Exam Topic 2)

The BEST key performance indicator (KPI) to measure the effectiveness of a vendor risk management program is the percentage of:

- A. vendors providing risk assessments on time.
- B. vendor contracts reviewed in the past year.
- C. vendor risk mitigation action items completed on time.
- D. vendors that have reported control-related incidents.

Answer: A

NEW QUESTION 678

- (Exam Topic 2)

A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

- A. strategy.
- B. profile.
- C. process.
- D. map.

Answer: A

NEW QUESTION 682

- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to ensure once a risk action plan has been completed?

- A. The risk owner has validated outcomes.
- B. The risk register has been updated.
- C. The control objectives are mapped to risk objectives.
- D. The requirements have been achieved.

Answer: B

NEW QUESTION 684

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?

- A. Self-assessments by process owners
- B. Mitigation plan progress reports
- C. Risk owner attestation
- D. Change in the level of residual risk

Answer: D

NEW QUESTION 686

- (Exam Topic 2)

The FIRST task when developing a business continuity plan should be to:

- A. determine data backup and recovery availability at an alternate site.
- B. identify critical business functions and resources.
- C. define roles and responsibilities for implementation.
- D. identify recovery time objectives (RTOs) for critical business applications.

Answer: B

NEW QUESTION 690

- (Exam Topic 2)

The BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability remediation program is the number of:

- A. vulnerability scans.
- B. recurring vulnerabilities.
- C. vulnerabilities remediated.
- D. new vulnerabilities identified.

Answer: C

NEW QUESTION 692

- (Exam Topic 2)

It is MOST important for a risk practitioner to have an awareness of an organization's processes in order to:

- A. perform a business impact analysis.
- B. identify potential sources of risk.
- C. establish risk guidelines.
- D. understand control design.

Answer: B

NEW QUESTION 694

- (Exam Topic 2)

What are the MOST important criteria to consider when developing a data classification scheme to facilitate risk assessment and the prioritization of risk mitigation activities?

- A. Mitigation and control value
- B. Volume and scope of data generated daily
- C. Business criticality and sensitivity
- D. Recovery point objective (RPO) and recovery time objective (RTO)

Answer: C

NEW QUESTION 698

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk responses have been executed according to their risk action plans?

- A. Risk policy review
- B. Business impact analysis (BIA)
- C. Control catalog
- D. Risk register

Answer: D

NEW QUESTION 701

- (Exam Topic 2)

What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium	Low	Low
Tango	Medium	Low	Medium
Uniform	High	High	High
Victor	High	Medium	Medium

- A. Relative positions on the risk map
- B. Risk treatment options
- C. Capability of enterprise to implement
- D. The multiple risk factors addressed by a chosen response

Answer: A

NEW QUESTION 704

- (Exam Topic 2)

As part of an overall IT risk management plan, an IT risk register BEST helps management:

- A. align IT processes with business objectives.
- B. communicate the enterprise risk management policy.
- C. stay current with existing control status.
- D. understand the organizational risk profile.

Answer: D

NEW QUESTION 709

- (Exam Topic 2)

Which of the following will BEST help to ensure that information system controls are effective?

- A. Responding promptly to control exceptions
- B. Implementing compensating controls
- C. Testing controls periodically
- D. Automating manual controls

Answer: C

NEW QUESTION 714

- (Exam Topic 2)

The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

- A. ensure policy and regulatory compliance.
- B. assess the proliferation of new threats.
- C. verify Internet firewall control settings.
- D. identify vulnerabilities in the system.

Answer: C

NEW QUESTION 719

- (Exam Topic 2)

The annualized loss expectancy (ALE) method of risk analysis:

- A. helps in calculating the expected cost of controls
- B. uses qualitative risk rankings such as low, medium and high.
- C. can be used in a cost-benefit analysis
- D. can be used to determine the indirect business impact.

Answer: C

NEW QUESTION 721

- (Exam Topic 2)

An IT risk practitioner is evaluating an organization's change management controls over the last six months. The GREATEST concern would be an increase in:

- A. rolled back changes below management's thresholds.
- B. change-related exceptions per month.
- C. the average implementation time for changes.
- D. number of user stories approved for implementation.

Answer: B

NEW QUESTION 723

- (Exam Topic 2)

Implementing which of the following will BEST help ensure that systems comply with an established baseline before deployment?

- A. Vulnerability scanning
- B. Continuous monitoring and alerting
- C. Configuration management
- D. Access controls and active logging

Answer: C

NEW QUESTION 724

- (Exam Topic 2)

A maturity model will BEST indicate:

- A. confidentiality and integrity.
- B. effectiveness and efficiency.
- C. availability and reliability.
- D. certification and accreditation.

Answer: B

NEW QUESTION 726

- (Exam Topic 2)

Which of the following is MOST helpful to review when identifying risk scenarios associated with the adoption of Internet of Things (IoT) technology in an organization?

- A. The business case for the use of IoT
- B. The IoT threat landscape
- C. Policy development for IoT
- D. The network that IoT devices can access

Answer: B

NEW QUESTION 731

- (Exam Topic 2)

Which of the following would qualify as a key performance indicator (KPI)?

- A. Aggregate risk of the organization
- B. Number of identified system vulnerabilities
- C. Number of exception requests processed in the past 90 days
- D. Number of attacks against the organization's website

Answer: B

NEW QUESTION 732

- (Exam Topic 2)

An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?

- A. Implement IT systems in alignment with business objectives.
- B. Review metrics and key performance indicators (KPIs).
- C. Review design documentation of IT systems.

D. Evaluate compliance with legal and regulatory requirements.

Answer: D

NEW QUESTION 735

- (Exam Topic 2)

Which of the following is the BEST way for a risk practitioner to verify that management has addressed control issues identified during a previous external audit?

- A. Interview control owners.
- B. Observe the control enhancements in operation.
- C. Inspect external audit documentation.
- D. Review management's detailed action plans.

Answer: B

NEW QUESTION 738

- (Exam Topic 2)

Which of the following should management consider when selecting a risk mitigation option?

- A. Maturity of the enterprise architecture
- B. Cost of control implementation
- C. Reliability of key performance indicators (KPIs)
- D. Reliability of key risk indicators (KPIs)

Answer: B

NEW QUESTION 739

- (Exam Topic 2)

Which of the following would be MOST beneficial as a key risk indicator (KRI)?

- A. Current capital allocation reserves
- B. Negative security return on investment (ROI)
- C. Project cost variances
- D. Annualized loss projections

Answer: D

NEW QUESTION 744

- (Exam Topic 2)

Within the three lines of defense model, the accountability for the system of internal control resides with:

- A. the chief information officer (CIO).
- B. the board of directors
- C. enterprise risk management
- D. the risk practitioner

Answer: B

NEW QUESTION 747

- (Exam Topic 2)

Which of the following should a risk practitioner do FIRST when an organization decides to use a cloud service?

- A. Review the vendor selection process and vetting criteria.
- B. Assess whether use of service falls within risk tolerance thresholds.
- C. Establish service level agreements (SLAs) with the vendor.
- D. Check the contract for appropriate security risk and control provisions.

Answer: D

NEW QUESTION 749

- (Exam Topic 2)

Who is responsible for IT security controls that are outsourced to an external service provider?

- A. Organization's information security manager
- B. Organization's risk function
- C. Service provider's IT management
- D. Service provider's information security manager

Answer: B

NEW QUESTION 752

- (Exam Topic 2)

Which of the following is the BEST indicator of the effectiveness of a control monitoring program?

- A. Time between control failure and failure detection

- B. Number of key controls as a percentage of total control count
- C. Time spent on internal control assessment reviews
- D. Number of internal control failures within the measurement period

Answer: A

NEW QUESTION 757

- (Exam Topic 2)

The BEST criteria when selecting a risk response is the:

- A. capability to implement the response
- B. importance of IT risk within the enterprise
- C. effectiveness of risk response options
- D. alignment of response to industry standards

Answer: C

NEW QUESTION 760

- (Exam Topic 2)

Which of the following would BEST enable mitigation of newly identified risk factors related to internet of Things (IoT)?

- A. Introducing control procedures early in the life cycle
- B. Implementing IoT device software monitoring
- C. Performing periodic risk assessments of IoT
- D. Performing secure code reviews

Answer: A

NEW QUESTION 764

- (Exam Topic 2)

To minimize risk in a software development project, when is the BEST time to conduct a risk analysis?

- A. During the business requirement definitions phase
- B. Before periodic steering committee meetings
- C. At each stage of the development life cycle
- D. During the business case development

Answer: A

NEW QUESTION 766

- (Exam Topic 2)

When establishing leading indicators for the information security incident response process it is MOST important to consider the percentage of reported incidents:

- A. that result in a full root cause analysis.
- B. used for verification within the SLA.
- C. that are verified as actual incidents.
- D. resolved within the SLA.

Answer: C

NEW QUESTION 770

- (Exam Topic 2)

Which of the following is MOST helpful in identifying gaps between the current and desired state of the IT risk environment?

- A. Analyzing risk appetite and tolerance levels
- B. Assessing identified risk and recording results in the risk register
- C. Evaluating risk scenarios and assessing current controls
- D. Reviewing guidance from industry best practices and standards

Answer: C

NEW QUESTION 775

- (Exam Topic 2)

Which of the following would MOST likely result in updates to an IT risk appetite statement?

- A. External audit findings
- B. Feedback from focus groups
- C. Self-assessment reports
- D. Changes in senior management

Answer: D

NEW QUESTION 780

- (Exam Topic 2)

Which of the following is the BEST course of action when risk is found to be above the acceptable risk appetite?

- A. Review risk tolerance levels
- B. Maintain the current controls.
- C. Analyze the effectiveness of controls.
- D. Execute the risk response plan

Answer: D

NEW QUESTION 782

- (Exam Topic 2)

Which of the following risk register elements is MOST likely to be updated if the attack surface or exposure of an asset is reduced?

- A. Likelihood rating
- B. Control effectiveness
- C. Assessment approach
- D. Impact rating

Answer: A

NEW QUESTION 785

- (Exam Topic 2)

Which of the following is the MOST important reason to create risk scenarios?

- A. To assist with risk identification
- B. To determine risk tolerance
- C. To determine risk appetite
- D. To assist in the development of risk responses

Answer: A

NEW QUESTION 789

- (Exam Topic 2)

An organization has outsourced its backup and recovery procedures to a third-party cloud provider. Which of the following is the risk practitioner's BEST course of action?

- A. Accept the risk and document contingency plans for data disruption.
- B. Remove the associated risk scenario from the risk register due to avoidance.
- C. Mitigate the risk with compensating controls enforced by the third-party cloud provider.
- D. Validate the transfer of risk and update the register to reflect the change.

Answer: C

NEW QUESTION 792

- (Exam Topic 2)

Business areas within an organization have engaged various cloud service providers directly without assistance from the IT department. What should the risk practitioner do?

- A. Recommend the IT department remove access to the cloud services.
- B. Engage with the business area managers to review controls applied.
- C. Escalate to the risk committee.
- D. Recommend a risk assessment be conducted.

Answer: B

NEW QUESTION 796

- (Exam Topic 2)

A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (PII). Which of the following will MOST likely outcome for an organization affected by the new law?

- A. Increase in compliance breaches
- B. Increase in loss event impact
- C. Increase in residual risk
- D. Increase in customer complaints

Answer: B

NEW QUESTION 799

- (Exam Topic 2)

Which of the following requirements is MOST important to include in an outsourcing contract to help ensure sensitive data stored with a service provider is secure?

- A. A third-party assessment report of control environment effectiveness must be provided at least annually.
- B. Incidents related to data loss must be reported to the organization immediately after they occur.
- C. Risk assessment results must be provided to the organization at least annually.
- D. A cyber insurance policy must be purchased to cover data loss events.

Answer: A

NEW QUESTION 803

- (Exam Topic 2)

The MAIN goal of the risk analysis process is to determine the:

- A. potential severity of impact
- B. frequency and magnitude of loss
- C. control deficiencies
- D. threats and vulnerabilities

Answer: B

NEW QUESTION 804

- (Exam Topic 2)

Which of the following is MOST important to understand when developing key risk indicators (KRIs)?

- A. KRI thresholds
- B. Integrity of the source data
- C. Control environment
- D. Stakeholder requirements

Answer: B

NEW QUESTION 806

- (Exam Topic 2)

The PRIMARY purpose of vulnerability assessments is to:

- A. provide clear evidence that the system is sufficiently secure.
- B. determine the impact of potential threats.
- C. test intrusion detection systems (IDS) and response procedures.
- D. detect weaknesses that could lead to system compromise.

Answer: D

NEW QUESTION 807

- (Exam Topic 2)

An organization has just implemented changes to close an identified vulnerability that impacted a critical business process. What should be the NEXT course of action?

- A. Redesign the heat map.
- B. Review the risk tolerance.
- C. Perform a business impact analysis (BIA)
- D. Update the risk register.

Answer: C

NEW QUESTION 812

- (Exam Topic 2)

Which of the following is MOST important for an organization to have in place when developing a risk management framework?

- A. A strategic approach to risk including an established risk appetite
- B. A risk-based internal audit plan for the organization
- C. A control function within the risk management team
- D. An organization-wide risk awareness training program

Answer: A

NEW QUESTION 816

- (Exam Topic 2)

An organization has outsourced its lease payment process to a service provider who lacks evidence of compliance with a necessary regulatory standard. Which risk treatment was adopted by the organization?

- A. Acceptance
- B. Transfer
- C. Mitigation
- D. Avoidance

Answer: A

NEW QUESTION 817

- (Exam Topic 2)

Which of the following is MOST important to include in a Software as a Service (SaaS) vendor agreement?

- A. An annual contract review
- B. A service level agreement (SLA)
- C. A requirement to adopt an established risk management framework
- D. A requirement to provide an independent audit report

Answer: B

NEW QUESTION 822

- (Exam Topic 2)

An IT license audit has revealed that there are several unlicensed copies of software to:

- A. immediately uninstall the unlicensed software from the laptops
- B. centralize administration rights on laptops so that installations are controlled
- C. report the issue to management so appropriate action can be taken.
- D. procure the requisite licenses for the software to minimize business impact.

Answer: B

NEW QUESTION 825

- (Exam Topic 2)

An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

- A. IT infrastructure head
- B. Human resources head
- C. Supplier management head
- D. Application development head

Answer: B

NEW QUESTION 827

- (Exam Topic 2)

When communicating changes in the IT risk profile, which of the following should be included to BEST enable stakeholder decision making?

- A. List of recent incidents affecting industry peers
- B. Results of external attacks and related compensating controls
- C. Gaps between current and desired states of the control environment
- D. Review of leading IT risk management practices within the industry

Answer: C

NEW QUESTION 832

- (Exam Topic 2)

A control owner has completed a year-long project to strengthen existing controls. It is MOST important for the risk practitioner to:

- A. update the risk register to reflect the correct level of residual risk.
- B. ensure risk monitoring for the project is initiated.
- C. conduct and document a business impact analysis (BIA).
- D. verify cost-benefit of the new controls being implemented.

Answer: A

NEW QUESTION 835

- (Exam Topic 2)

A risk practitioner observes that the fraud detection controls in an online payment system do not perform as expected. Which of the following will MOST likely change as a result?

- A. Impact
- B. Residual risk
- C. Inherent risk
- D. Risk appetite

Answer: B

NEW QUESTION 840

- (Exam Topic 2)

Who is MOST likely to be responsible for the coordination between the IT risk strategy and the business risk strategy?

- A. Chief financial officer
- B. Information security director
- C. Internal audit director
- D. Chief information officer

Answer: B

NEW QUESTION 845

- (Exam Topic 2)

Which of the following is MOST effective in continuous risk management process improvement?

- A. Periodic assessments
- B. Change management

- C. Awareness training
- D. Policy updates

Answer: A

NEW QUESTION 846

- (Exam Topic 2)

The MAIN purpose of having a documented risk profile is to:

- A. comply with external and internal requirements.
- B. enable well-informed decision making.
- C. prioritize investment projects.
- D. keep the risk register up-to-date.

Answer: B

NEW QUESTION 850

- (Exam Topic 2)

An identified high probability risk scenario involving a critical, proprietary business function has an annualized cost of control higher than the annual loss expectancy. Which of the following is the BEST risk response?

- A. Mitigate
- B. Accept
- C. Transfer
- D. Avoid

Answer: B

NEW QUESTION 854

- (Exam Topic 2)

A bank has outsourced its statement printing function to an external service provider. Which of the following is the MOST critical requirement to include in the contract?

- A. Monitoring of service costs
- B. Provision of internal audit reports
- C. Notification of sub-contracting arrangements
- D. Confidentiality of customer data

Answer: D

NEW QUESTION 856

- (Exam Topic 2)

Which of the following should be the risk practitioner's FIRST course of action when an organization has decided to expand into new product areas?

- A. Identify any new business objectives with stakeholders.
- B. Present a business case for new controls to stakeholders.
- C. Revise the organization's risk and control policy.
- D. Review existing risk scenarios with stakeholders.

Answer: D

NEW QUESTION 860

- (Exam Topic 2)

An organization's financial analysis department uses an in-house forecasting application for business projections. Who is responsible for defining access roles to protect the sensitive data within this application?

- A. IT risk manager
- B. IT system owner
- C. Information security manager
- D. Business owner

Answer: D

NEW QUESTION 861

- (Exam Topic 2)

Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?

- A. Establishing a risk management committee
- B. Updating the organization's risk register to reflect the new threat
- C. Communicating the results of the threat impact analysis
- D. Establishing metrics to assess the effectiveness of the responses

Answer: C

NEW QUESTION 864

- (Exam Topic 2)

Which of the following would be of GREATEST assistance when justifying investment in risk response strategies?

- A. Total cost of ownership
- B. Resource dependency analysis
- C. Cost-benefit analysis
- D. Business impact analysis

Answer: C

NEW QUESTION 866

- (Exam Topic 2)

An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

- A. Number of customer records held
- B. Number of databases that host customer data
- C. Number of encrypted customer databases
- D. Number of staff members having access to customer data

Answer: B

NEW QUESTION 871

- (Exam Topic 2)

A risk practitioner has been notified that an employee sent an email in error containing customers' personally identifiable information (PII). Which of the following is the risk practitioner's BEST course of action?

- A. Report it to the chief risk officer.
- B. Advise the employee to forward the email to the phishing team.
- C. follow incident reporting procedures.
- D. Advise the employee to permanently delete the email.

Answer: C

NEW QUESTION 875

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CRISC Practice Exam Features:

- * CRISC Questions and Answers Updated Frequently
- * CRISC Practice Questions Verified by Expert Senior Certified Staff
- * CRISC Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CRISC Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CRISC Practice Test Here](#)