

Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control



NEW QUESTION 1

- (Exam Topic 4)

A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?

- A. Develop a mechanism for monitoring residual risk.
- B. Update the risk register with the results.
- C. Prepare a business case for the response options.
- D. Identify resources for implementing responses.

Answer: C

NEW QUESTION 2

- (Exam Topic 4)

When classifying and prioritizing risk responses, the areas to address FIRST are those with:

- A. low cost effectiveness ratios and high risk levels
- B. high cost effectiveness ratios and low risk levels.
- C. high cost effectiveness ratios and high risk levels
- D. low cost effectiveness ratios and low risk levels.

Answer: C

NEW QUESTION 3

- (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 4

- (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 5

- (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 6

- (Exam Topic 4)

A risk practitioner has collaborated with subject matter experts from the IT department to develop a large list of potential key risk indicators (KRIs) for all IT operations within the organization. Of the following, who should review the completed list and select the appropriate KRIs for implementation?

- A. IT security managers
- B. IT control owners
- C. IT auditors
- D. IT risk owners

Answer: D

NEW QUESTION 7

- (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 8

- (Exam Topic 4)

Which of the following is the BEST way to ensure data is properly sanitized while in cloud storage?

- A. Deleting the data from the file system
- B. Cryptographically scrambling the data
- C. Formatting the cloud storage at the block level
- D. Degaussing the cloud storage media

Answer: B

NEW QUESTION 9

- (Exam Topic 4)

An organization's business gap analysis reveals the need for a robust IT risk strategy. Which of the following should be the risk practitioner's PRIMARY consideration when participating in development of the new strategy?

- A. Scale of technology
- B. Risk indicators
- C. Risk culture
- D. Proposed risk budget

Answer: C

NEW QUESTION 10

- (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 10

- (Exam Topic 4)

Which of the following is the MOST important information to cover a business continuity awareness training program for all employees of the organization?

- A. Recovery time objectives (RTOs)
- B. Segregation of duties
- C. Communication plan
- D. Critical asset inventory

Answer: C

NEW QUESTION 15

- (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 20

- (Exam Topic 4)

The MOST important measure of the effectiveness of risk management in project implementation is the percentage of projects:

- A. introduced into production without high-risk issues.
- B. having the risk register updated regularly.
- C. having key risk indicators (KRIs) established to measure risk.
- D. having an action plan to remediate overdue issues.

Answer: A

NEW QUESTION 24

- (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 25

- (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 27

- (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 30

- (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 33

- (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 36

- (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 38

- (Exam Topic 4)

An organization's control environment is MOST effective when:

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

Answer: A

NEW QUESTION 42

- (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 43

- (Exam Topic 4)

Which of the following, who should be PRIMARILY responsible for performing user entitlement reviews?

- A. IT security manager
- B. IT personnel
- C. Data custodian
- D. Data owner

Answer: D

NEW QUESTION 44

- (Exam Topic 4)

Which of the following should be the FIRST consideration when establishing a new risk governance program?

- A. Developing an ongoing awareness and training program
- B. Creating policies and standards that are easy to comprehend
- C. Embedding risk management into the organization
- D. Completing annual risk assessments on critical resources

Answer: B

NEW QUESTION 45

- (Exam Topic 4)

A root cause analysis indicates a major service disruption due to a lack of competency of newly hired IT system administrators. Who should be accountable for resolving the situation?

- A. HR training director
- B. Business process owner
- C. HR recruitment manager
- D. Chief information officer (CIO)

Answer: C

NEW QUESTION 50

- (Exam Topic 4)

If preventive controls cannot be implemented due to technology limitations, which of the following should be done FIRST to reduce risk?

- A. Evaluate alternative controls.
- B. Redefine the business process to reduce the risk.
- C. Develop a plan to upgrade technology.
- D. Define a process for monitoring risk.

Answer: A

NEW QUESTION 52

- (Exam Topic 4)

Which of the following would be a risk practitioner's GREATEST concern with the use of a vulnerability scanning tool?

- A. Increased time to remediate vulnerabilities
- B. Inaccurate reporting of results
- C. Increased number of vulnerabilities
- D. Network performance degradation

Answer: B

NEW QUESTION 56

- (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 activities
- B. The maximum levels of applicable regulatory fines
- C. The length of time between identification and containment of the incident
- D. The composition and number of records in the information asset

Answer:

C

NEW QUESTION 58

- (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 63

- (Exam Topic 4)

Which of the following is the BEST approach for an organization in a heavily regulated industry to comprehensively test application functionality?

- A. Use production data in a non-production environment
- B. Use masked data in a non-production environment
- C. Use test data in a production environment
- D. Use anonymized data in a non-production environment

Answer: D

NEW QUESTION 67

- (Exam Topic 4)

When is the BEST to identify risk associated with major project to determine a mitigation plan?

- A. Project execution phase
- B. Project initiation phase
- C. Project closing phase
- D. Project planning phase

Answer: D

NEW QUESTION 69

- (Exam Topic 4)

Which of the following is the BEST way to validate whether controls to reduce user device vulnerabilities have been implemented according to management's action plan?

- A. Survey device owners.
- B. Rescan the user environment.
- C. Require annual end user policy acceptance.
- D. Review awareness training assessment results

Answer: B

NEW QUESTION 71

- (Exam Topic 4)

A multinational organization is considering implementing standard background checks to all new employees. A KEY concern regarding this approach

- A. fail to identify all relevant issues.
- B. be too costly
- C. violate laws in other countries
- D. be too time consuming

Answer: C

NEW QUESTION 75

- (Exam Topic 3)

Which of the following should be of GREATEST concern for an organization considering the adoption of a bring your own device (BYOD) initiative?

- A. Device corruption
- B. Data loss
- C. Malicious users
- D. User support

Answer: B

NEW QUESTION 79

- (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 80

- (Exam Topic 4)

A recent big data project has resulted in the creation of an application used to support important investment decisions. Which of the following should be of GREATEST concern to the risk practitioner?

- A. Data quality
- B. Maintenance costs
- C. Data redundancy
- D. System integration

Answer: A

NEW QUESTION 85

- (Exam Topic 4)

Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?

- A. Fiscal management practices
- B. Business maturity
- C. Budget for implementing security
- D. Management culture

Answer: D

NEW QUESTION 88

- (Exam Topic 4)

Which of the following would MOST likely cause management to unknowingly accept excessive risk?

- A. Satisfactory audit results
- B. Risk tolerance being set too low
- C. Inaccurate risk ratings
- D. Lack of preventive controls

Answer: C

NEW QUESTION 90

- (Exam Topic 4)

An organization has allowed several employees to retire early in order to avoid layoffs. Many of these employees have been subject matter experts for critical assets. Which type of risk is MOST likely to materialize?

- A. Confidentiality breach
- B. Institutional knowledge loss
- C. Intellectual property loss
- D. Unauthorized access

Answer: B

NEW QUESTION 92

- (Exam Topic 4)

A penetration test reveals several vulnerabilities in a web-facing application. Which of the following should be the FIRST step in selecting a risk response?

- A. Correct the vulnerabilities to mitigate potential risk exposure.
- B. Develop a risk response action plan with key stakeholders.
- C. Assess the level of risk associated with the vulnerabilities.
- D. Communicate the vulnerabilities to the risk owner.

Answer: C

NEW QUESTION 95

- (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 99

- (Exam Topic 4)

Which of the following resources is MOST helpful to a risk practitioner when updating the likelihood rating in the risk register?

- A. Risk control assessment
- B. Audit reports with risk ratings
- C. Penetration test results
- D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 102

- (Exam Topic 3)

An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course of action?

- A. Report the observation to the chief risk officer (CRO).
- B. Validate the adequacy of the implemented risk mitigation measures.
- C. Update the risk register with the implemented risk mitigation actions.
- D. Revert the implemented mitigation measures until approval is obtained

Answer: B

NEW QUESTION 103

- (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 108

- (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 112

- (Exam Topic 3)

During a risk treatment plan review, a risk practitioner finds the approved risk action plan has not been completed. However, there were other risk mitigation actions implemented. Which of the following is the BEST course of action?

- A. Review the cost-benefit of mitigating controls
- B. Mark the risk status as unresolved within the risk register
- C. Verify the sufficiency of mitigating controls with the risk owner
- D. Update the risk register with implemented mitigating actions

Answer: A

NEW QUESTION 117

- (Exam Topic 3)

An organization has initiated a project to launch an IT-based service to customers and take advantage of being the first to market. Which of the following should be of GREATEST concern to senior management?

- A. More time has been allotted for testing.
- B. The project is likely to deliver the product late.
- C. A new project manager is handling the project.
- D. The cost of the project will exceed the allotted budget.

Answer: B

NEW QUESTION 120

- (Exam Topic 3)

A financial institution has identified high risk of fraud in several business applications. Which of the following controls will BEST help reduce the risk of fraudulent internal transactions?

- A. Periodic user privileges review
- B. Log monitoring
- C. Periodic internal audits
- D. Segregation of duties

Answer: A

NEW QUESTION 125

- (Exam Topic 3)

When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

- A. business process objectives have been met.
- B. control adheres to regulatory standards.
- C. residual risk objectives have been achieved.
- D. control process is designed effectively.

Answer: D

NEW QUESTION 129

- (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 131

- (Exam Topic 3)

The PRIMARY benefit associated with key risk indicators (KRIs) is that they:

- A. help an organization identify emerging threats.
- B. benchmark the organization's risk profile.
- C. identify trends in the organization's vulnerabilities.
- D. enable ongoing monitoring of emerging risk.

Answer: D

NEW QUESTION 136

- (Exam Topic 3)

Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

- A. Vulnerability scanning
- B. Systems log correlation analysis
- C. Penetration testing
- D. Monitoring of intrusion detection system (IDS) alerts

Answer: C

NEW QUESTION 140

- (Exam Topic 3)

Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

- A. Percentage of business users completing risk training
- B. Percentage of high-risk scenarios for which risk action plans have been developed
- C. Number of key risk indicators (KRIs) defined
- D. Time between when IT risk scenarios are identified and the enterprise's response

Answer: B

NEW QUESTION 144

- (Exam Topic 3)

A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

- A. Regulatory requirements may differ in each country.
- B. Data sampling may be impacted by various industry restrictions.
- C. Business advertising will need to be tailored by country.
- D. The data analysis may be ineffective in achieving objectives.

Answer: A

NEW QUESTION 146

- (Exam Topic 3)

Which of the following will help ensure the elective decision-making of an IT risk management committee?

- A. Key stakeholders are enrolled as members

- B. Approved minutes are forwarded to senior management
- C. Committee meets at least quarterly
- D. Functional overlap across the business is minimized

Answer: D

NEW QUESTION 148

- (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 152

- (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 154

- (Exam Topic 3)

The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:

- A. changes due to emergencies.
- B. changes that cause incidents.
- C. changes not requiring user acceptance testing.
- D. personnel that have rights to make changes in production.

Answer: B

NEW QUESTION 157

- (Exam Topic 3)

Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?

- A. Evaluating the impact to control objectives
- B. Conducting a root cause analysis
- C. Validating the adequacy of current processes
- D. Reconfiguring the IT infrastructure

Answer: B

NEW QUESTION 159

- (Exam Topic 3)

Which of the following is the MOST important topic to cover in a risk awareness training program for all staff?

- A. Internal and external information security incidents
- B. The risk department's roles and responsibilities
- C. Policy compliance requirements and exceptions process
- D. The organization's information security risk profile

Answer: C

NEW QUESTION 161

- (Exam Topic 3)

Which of the following is the MOST important responsibility of a risk owner?

- A. Testing control design
- B. Accepting residual risk
- C. Establishing business information criteria
- D. Establishing the risk register

Answer: C

NEW QUESTION 162

- (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 164

- (Exam Topic 3)

Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

- A. Conduct an abbreviated version of the assessment.
- B. Report the business unit manager for a possible ethics violation.
- C. Perform the assessment as it would normally be done.
- D. Recommend an internal auditor perform the review.

Answer: B

NEW QUESTION 166

- (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 169

- (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 170

- (Exam Topic 3)

Which of the following should be the GREATEST concern for an organization that uses open source software applications?

- A. Lack of organizational policy regarding open source software
- B. Lack of reliability associated with the use of open source software
- C. Lack of monitoring over installation of open source software in the organization
- D. Lack of professional support for open source software

Answer: A

NEW QUESTION 174

- (Exam Topic 3)

Which of the following is the MOST appropriate action when a tolerance threshold is exceeded?

- A. Communicate potential impact to decision makers.
- B. Research the root cause of similar incidents.
- C. Verify the response plan is adequate.
- D. Increase human resources to respond in the interim.

Answer: A

NEW QUESTION 177

- (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 180

- (Exam Topic 3)

Which of the following is the PRIMARY risk management responsibility of the second line of defense?

- A. Monitoring risk responses
- B. Applying risk treatments
- C. Providing assurance of control effectiveness
- D. Implementing internal controls

Answer: A

NEW QUESTION 182

- (Exam Topic 3)

Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

- A. Implement controls to bring the risk to a level within appetite and accept the residual risk.
- B. Implement a key performance indicator (KPI) to monitor the existing control performance.
- C. Accept the residual risk in its entirety and obtain executive management approval.
- D. Separate the risk into multiple components and avoid the risk components that cannot be mitigated.

Answer: C

NEW QUESTION 186

- (Exam Topic 3)

Which of the following represents a vulnerability?

- A. An identity thief seeking to acquire personal financial data from an organization
- B. Media recognition of an organization's market leadership in its industry
- C. A standard procedure for applying software patches two weeks after release
- D. An employee recently fired for insubordination

Answer: C

NEW QUESTION 188

- (Exam Topic 3)

Which of the following is MOST important for an organization to update following a change in legislation requiring notification to individuals impacted by data breaches?

- A. Insurance coverage
- B. Security awareness training
- C. Policies and standards
- D. Risk appetite and tolerance

Answer: C

NEW QUESTION 191

- (Exam Topic 3)

When performing a risk assessment of a new service to support a new Business process, which of the following should be done FIRST to ensure continuity of operations?

- A. Identify conditions that may cause disruptions
- B. Review incident response procedures
- C. Evaluate the probability of risk events
- D. Define metrics for restoring availability

Answer: A

NEW QUESTION 193

- (Exam Topic 3)

Which of the following should be determined FIRST when a new security vulnerability is made public?

- A. Whether the affected technology is used within the organization
- B. Whether the affected technology is Internet-facing
- C. What mitigating controls are currently in place
- D. How pervasive the vulnerability is within the organization

Answer: A

NEW QUESTION 194

- (Exam Topic 3)

Which 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 197

- (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 198

- (Exam Topic 3)

An organization discovers significant vulnerabilities in a recently purchased commercial off-the-shelf software product which will not be corrected until the next release. Which of the following is the risk manager's BEST course of action?

- A. Review the risk of implementing versus postponing with stakeholders.
- B. Run vulnerability testing tools to independently verify the vulnerabilities.
- C. Review software license to determine the vendor's responsibility regarding vulnerabilities.
- D. Require the vendor to correct significant vulnerabilities prior to installation.

Answer: C

NEW QUESTION 203

- (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 205

- (Exam Topic 3)

Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

- A. The sum of residual risk levels for each scenario
- B. The loss expectancy for aggregated risk scenarios
- C. The highest loss expectancy among the risk scenarios
- D. The average of anticipated residual risk levels

Answer: D

NEW QUESTION 210

- (Exam Topic 3)

An internal audit report reveals that not all IT application databases have encryption in place. Which of the following information would be MOST important for assessing the risk impact?

- A. The number of users who can access sensitive data
- B. A list of unencrypted databases which contain sensitive data
- C. The reason some databases have not been encrypted
- D. The cost required to enforce encryption

Answer: B

NEW QUESTION 212

- (Exam Topic 3)

Who should have the authority to approve an exception to a control?

- A. information security manager
- B. Control owner
- C. Risk owner
- D. Risk manager

Answer: C

NEW QUESTION 215

- (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 217

- (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 218

- (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 223

- (Exam Topic 3)

During implementation of an intrusion detection system (IDS) to monitor network traffic, a high number of alerts is reported. The risk practitioner should recommend to:

- A. reset the alert threshold based on peak traffic
- B. analyze the traffic to minimize the false negatives
- C. analyze the alerts to minimize the false positives
- D. sniff the traffic using a network analyzer

Answer: C

NEW QUESTION 228

- (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 231

- (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 235

- (Exam Topic 3)

A risk practitioner identifies a database application that has been developed and implemented by the business independently of IT. Which of the following is the BEST course of action?

- A. Escalate the concern to senior management.
- B. Document the reasons for the exception.
- C. Include the application in IT risk assessments.
- D. Propose that the application be transferred to IT.

Answer: B

NEW QUESTION 238

- (Exam Topic 3)

Which of the following criteria associated with key risk indicators (KRIs) BEST enables effective risk monitoring?

- A. Approval by senior management
- B. Low cost of development and maintenance
- C. Sensitivity to changes in risk levels
- D. Use of industry risk data sources

Answer: C

NEW QUESTION 240

- (Exam Topic 3)

The BEST way to obtain senior management support for investment in a control implementation would be to articulate the reduction in:

- A. detected incidents.
- B. residual risk.
- C. vulnerabilities.
- D. inherent risk.

Answer: D

NEW QUESTION 244

- (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 249

- (Exam Topic 3)

Which of the following BEST enables the identification of trends in risk levels?

- A. Correlation between risk levels and key risk indicators (KRIs) is positive.
- B. Measurements for key risk indicators (KRIs) are repeatable
- C. Quantitative measurements are used for key risk indicators (KRIs).
- D. Qualitative definitions for key risk indicators (KRIs) are used.

Answer: B

NEW QUESTION 250

- (Exam Topic 3)

Which of the following is the PRIMARY reason to use key control indicators (KCIs) to evaluate control operating effectiveness?

- A. To measure business exposure to risk
- B. To identify control vulnerabilities
- C. To monitor the achievement of set objectives
- D. To raise awareness of operational issues

Answer: C

NEW QUESTION 251

- (Exam Topic 3)

Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:

- A. is in charge of information security.
- B. is responsible for enterprise risk management (ERM)
- C. can implement remediation action plans.
- D. is accountable for loss if the risk materializes.

Answer: D

NEW QUESTION 252

- (Exam Topic 3)

Reviewing historical risk events is MOST useful for which of the following processes within the risk management life cycle?

- A. Risk monitoring
- B. Risk mitigation
- C. Risk aggregation

D. Risk assessment

Answer: D

NEW QUESTION 255

- (Exam Topic 3)

Vulnerabilities have been detected on an organization's systems. Applications installed on these systems will not operate if the underlying servers are updated. Which of the following is the risk practitioner's BEST course of action?

- A. Recommend the business change the application.
- B. Recommend a risk treatment plan.
- C. Include the risk in the next quarterly update to management.
- D. Implement compensating controls.

Answer: D

NEW QUESTION 260

- (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 265

- (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 269

- (Exam Topic 3)

Which of the following is the MOST important reason to link an effective key control indicator (KCI) to relevant key risk indicators (KRIs)?

- A. To monitor changes in the risk environment
- B. To provide input to management for the adjustment of risk appetite
- C. To monitor the accuracy of threshold levels in metrics
- D. To obtain business buy-in for investment in risk mitigation measures

Answer: A

NEW QUESTION 274

- (Exam Topic 3)

Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?

- A. Segregation of duties
- B. Three lines of defense
- C. Compliance review
- D. Quality assurance review

Answer: B

NEW QUESTION 278

- (Exam Topic 3)

Which of the following provides the MOST useful information to determine risk exposure following control implementations?

- A. Strategic plan and risk management integration
- B. Risk escalation and process for communication
- C. Risk limits, thresholds, and indicators
- D. Policies, standards, and procedures

Answer: C

NEW QUESTION 281

- (Exam Topic 3)

Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?

- A. Ensuring that database changes are correctly applied
- B. Enforcing that changes are authorized
- C. Deterring illicit actions of database administrators
- D. Preventing system developers from accessing production data

Answer: C

NEW QUESTION 282

- (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 285

- (Exam Topic 3)

Which of the following key control indicators (KCIs) BEST indicates whether security requirements are identified and managed throughout a project life cycle?

- A. Number of projects going live without a security review
- B. Number of employees completing project-specific security training
- C. Number of security projects started in core departments
- D. Number of security-related status reports submitted by project managers

Answer: A

NEW QUESTION 290

- (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 292

- (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 296

- (Exam Topic 3)

Which of the following practices MOST effectively safeguards the processing of personal data?

- A. Personal data attributed to a specific data subject is tokenized.
- B. Data protection impact assessments are performed on a regular basis.
- C. Personal data certifications are performed to prevent excessive data collection.
- D. Data retention guidelines are documented, established, and enforced.

Answer: B

NEW QUESTION 300

- (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 304

- (Exam Topic 3)

Which of the following should be management's PRIMARY consideration when approving risk response action plans?

- A. Ability of the action plans to address multiple risk scenarios
- B. Ease of implementing the risk treatment solution
- C. Changes in residual risk after implementing the plans
- D. Prioritization for implementing the action plans

Answer: C

NEW QUESTION 307

- (Exam Topic 3)

Which of the following will be MOST effective in uniquely identifying the originator of electronic transactions?

- A. Digital signature
- B. Edit checks
- C. Encryption
- D. Multifactor authentication

Answer: A

NEW QUESTION 309

- (Exam Topic 3)

Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

- A. Financial risk is given a higher priority.
- B. Risk with strategic impact is included.
- C. Security strategy is given a higher priority.
- D. Risk identified by industry benchmarking is included.

Answer: B

NEW QUESTION 311

- (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 313

- (Exam Topic 3)

Legal and regulatory risk associated with business conducted over the Internet is driven by:

- A. the jurisdiction in which an organization has its principal headquarters
- B. international law and a uniform set of regulations.
- C. the laws and regulations of each individual country
- D. international standard-setting bodies.

Answer: C

NEW QUESTION 314

- (Exam Topic 3)

Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

- A. Customer database manager
- B. Customer data custodian
- C. Data privacy officer
- D. Audit committee

Answer: B

NEW QUESTION 317

- (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 320

- (Exam Topic 3)

An organization outsources the processing of its payroll data. A risk practitioner identifies a control weakness at the third party that exposes the payroll data. Who should own this risk?

- A. The third party's IT operations manager
- B. The organization's process owner
- C. The third party's chief risk officer (CRO)
- D. The organization's risk practitioner

Answer: B

NEW QUESTION 325

- (Exam Topic 3)

Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?

- A. Ongoing availability of data
- B. Ability to aggregate data
- C. Ability to predict trends
- D. Availability of automated reporting systems

Answer: D

NEW QUESTION 330

- (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 333

- (Exam Topic 3)

Which of the following is MOST important to the integrity of a security log?

- A. Least privilege access
- B. Inability to edit
- C. Ability to overwrite
- D. Encryption

Answer: B

NEW QUESTION 334

- (Exam Topic 3)

Which of the following is the MOST important consideration when sharing risk management updates with executive management?

- A. Including trend analysis of risk metrics
- B. Using an aggregated view of organizational risk
- C. Relying on key risk indicator (KRI) data
- D. Ensuring relevance to organizational goals

Answer: D

NEW QUESTION 339

- (Exam Topic 3)

The PRIMARY advantage of involving end users in continuity planning is that they:

- A. have a better understanding of specific business needs
- B. can balance the overall technical and business concerns
- C. can see the overall impact to the business
- D. are more objective than information security management.

Answer: B

NEW QUESTION 342

- (Exam Topic 3)

What is the PRIMARY benefit of risk monitoring?

- A. It reduces the number of audit findings.
- B. It provides statistical evidence of control efficiency.
- C. It facilitates risk-aware decision making.
- D. It facilitates communication of threat levels.

Answer:

C

NEW QUESTION 345

- (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 346

- (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 350

- (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 352

- (Exam Topic 3)

Which of the following would be MOST useful to senior management when determining an appropriate risk response?

- A. A comparison of current risk levels with established tolerance
- B. A comparison of cost variance with defined response strategies
- C. A comparison of current risk levels with estimated inherent risk levels
- D. A comparison of accepted risk scenarios associated with regulatory compliance

Answer: A

NEW QUESTION 353

- (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 358

- (Exam Topic 3)

Analyzing trends in key control indicators (KCI) 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 362

- (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 367

- (Exam Topic 3)

Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

- A. Conducting a business impact analysis (BIA)
- B. Identifying the recovery response team
- C. Procuring a recovery site
- D. Assigning sensitivity levels to data

Answer: A

NEW QUESTION 370

- (Exam Topic 3)

When formulating a social media policy to address information leakage, which of the following is the MOST important concern to address?

- A. Sharing company information on social media
- B. Sharing personal information on social media
- C. Using social media to maintain contact with business associates
- D. Using social media for personal purposes during working hours

Answer: A

NEW QUESTION 375

- (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 380

- (Exam Topic 3)

Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

- A. To enable consistent data on risk to be obtained
- B. To allow for proper review of risk tolerance
- C. To identify dependencies for reporting risk
- D. To provide consistent and clear terminology

Answer: B

NEW QUESTION 384

- (Exam Topic 3)

Which of the following issues should be of GREATEST concern when evaluating existing controls during a risk assessment?

- A. A high number of approved exceptions exist with compensating controls.
- B. Successive assessments have the same recurring vulnerabilities.
- C. Redundant compensating controls are in place.
- D. Asset custodians are responsible for defining controls instead of asset owners.

Answer: B

NEW QUESTION 385

- (Exam Topic 3)

To communicate the risk associated with IT in business terms, which of the following MUST be defined?

- A. Compliance objectives
- B. Risk appetite of the organization
- C. Organizational objectives
- D. Inherent and residual risk

Answer: C

NEW QUESTION 388

- (Exam Topic 3)

Which of the following approaches BEST identifies information systems control deficiencies?

- A. Countermeasures analysis

- B. Best practice assessment
- C. Gap analysis
- D. Risk assessment

Answer: C

NEW QUESTION 391

- (Exam Topic 3)

Which of The following is the MOST comprehensive input to the risk assessment process specific to the effects of system downtime?

- A. Business continuity plan (BCP) testing results
- B. Recovery lime objective (RTO)
- C. Business impact analysis (BIA)
- D. results Recovery point objective (RPO)

Answer: C

NEW QUESTION 396

- (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 397

- (Exam Topic 3)

Which of the following BEST enables an organization to determine whether external emerging risk factors will impact the organization's risk profile?

- A. Control identification and mitigation
- B. Adoption of a compliance-based approach
- C. Prevention and detection techniques
- D. Scenario analysis and stress testing

Answer: D

NEW QUESTION 401

- (Exam Topic 3)

In which of the following system development life cycle (SDLC) phases should controls be incorporated into system specifications?

- A. Implementation
- B. Development
- C. Design
- D. Feasibility

Answer: C

NEW QUESTION 402

- (Exam Topic 3)

Which of the following is the BEST way to quantify the likelihood of risk materialization?

- A. Balanced scorecard
- B. Threat and vulnerability assessment
- C. Compliance assessments
- D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 407

- (Exam Topic 3)

A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

- A. Single sign-on
- B. Audit trail review
- C. Multi-factor authentication
- D. Data encryption at rest

Answer: B

NEW QUESTION 408

- (Exam Topic 3)

Which of the following would be MOST helpful when communicating roles associated with the IT risk management process?

- A. Skills matrix
- B. Job descriptions
- C. RACI chart
- D. Organizational chart

Answer: A

NEW QUESTION 410

- (Exam Topic 3)

An organization has outsourced its billing function to an external service provider. Who should own the risk of customer data leakage caused by the service provider?

- A. The service provider
- B. Vendor risk manager
- C. Legal counsel
- D. Business process owner

Answer: D

NEW QUESTION 413

- (Exam Topic 3)

Days before the realization of an acquisition, a data breach is discovered at the company to be acquired. For the accruing organization, this situation represents which of the following?

- A. Threat event
- B. Inherent risk
- C. Risk event
- D. Security incident

Answer: B

NEW QUESTION 414

- (Exam Topic 3)

Which of the following is the MOST effective control to address the risk associated with compromising data privacy within the cloud?

- A. Establish baseline security configurations with the cloud service provider.
- B. Require the cloud provider to disclose past data privacy breaches.
- C. Ensure the cloud service provider performs an annual risk assessment.
- D. Specify cloud service provider liability for data privacy breaches in the contract

Answer: D

NEW QUESTION 416

- (Exam Topic 3)

In an organization where each division manages risk independently, which of the following would BEST enable management of risk at the enterprise level?

- A. A standardized risk taxonomy
- B. A list of control deficiencies
- C. An enterprise risk ownership policy
- D. An updated risk tolerance metric

Answer: A

NEW QUESTION 417

- (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 418

- (Exam Topic 4)

Which of the following is the MOST important characteristic of a key risk indicator (KRI) to enable decision-making?

- A. Monitoring the risk until the exposure is reduced
- B. Setting minimum sample sizes to ensure accuracy
- C. Listing alternative causes for risk events
- D. Illustrating changes in risk trends

Answer: D

NEW QUESTION 423

- (Exam Topic 4)

Senior management is deciding whether to share confidential data with the organization's business partners. The BEST course of action for a risk practitioner would be to submit a report to senior management containing the:

- A. possible risk and suggested mitigation plans.
- B. design of controls to encrypt the data to be shared.
- C. project plan for classification of the data.
- D. summary of data protection and privacy legislation.

Answer: A

NEW QUESTION 424

- (Exam Topic 4)

Which of the following BEST balances the costs and benefits of managing IT risk*?

- A. Prioritizing and addressing risk in line with risk appetit
- B. Eliminating risk through preventive and detective controls
- C. Considering risk that can be shared with a third party
- D. Evaluating the probability and impact of risk scenarios

Answer: A

NEW QUESTION 428

- (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 430

- (Exam Topic 4)

Which of the following BEST enables a risk practitioner to understand management's approach to organizational risk?

- A. Organizational structure and job descriptions
- B. Risk appetite and risk tolerance
- C. Industry best practices for risk management
- D. Prior year's risk assessment results

Answer: B

NEW QUESTION 433

- (Exam Topic 4)

Which of the following will BEST help to ensure the continued effectiveness of the IT risk management function within an organization experiencing high employee turnover?

- A. Well documented policies and procedures
- B. Risk and issue tracking
- C. An IT strategy committee
- D. Change and release management

Answer: B

NEW QUESTION 437

- (Exam Topic 4)

An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

- A. Management may be unable to accurately evaluate the risk profile.
- B. Resources may be inefficiently allocated.
- C. The same risk factor may be identified in multiple areas.
- D. Multiple risk treatment efforts may be initiated to treat a given risk.

Answer: A

NEW QUESTION 439

- (Exam Topic 4)

Which of the following provides the MOST useful information to assess the magnitude of identified deficiencies in the IT control environment?

- A. Peer benchmarks
- B. Internal audit reports
- C. Business impact analysis (BIA) results
- D. Threat analysis results

Answer: D

NEW QUESTION 444

- (Exam Topic 4)

Which of the following BEST enables senior management to compare the ratings of risk scenarios?

- A. Key risk indicators (KRIs)
- B. Key performance indicators (KPIs)
- C. Control self-assessment (CSA)
- D. Risk heat map

Answer: D

NEW QUESTION 448

- (Exam Topic 4)

Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board?"

- A. A summary of risk response plans with validation results
- B. A report with control environment assessment results
- C. A dashboard summarizing key risk indicators (KRIs)
- D. A summary of IT risk scenarios with business cases

Answer: C

NEW QUESTION 449

- (Exam Topic 4)

Who should be responsible (of evaluating the residual risk after a compensating control has been

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

Answer: D

NEW QUESTION 453

- (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 454

- (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 455

- (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 456

- (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 461

- (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 464

- (Exam Topic 4)

An organization is planning to move its application infrastructure from on-premises to the cloud. Which of the following is the BEST course of the action to address the risk associated with data transfer if the relationship is terminated with the vendor?

- A. Meet with the business leaders to ensure the classification of their transferred data is in place
- B. Ensure the language in the contract explicitly states who is accountable for each step of the data transfer process
- C. Collect requirements for the environment to ensure the infrastructure as a service (IaaS) is configured appropriately.
- D. Work closely with the information security officer to ensure the company has the proper security controls in place.

Answer: B

NEW QUESTION 468

- (Exam Topic 4)

An incentive program is MOST likely implemented to manage the risk associated with loss of which organizational asset?

- A. Employees
- B. Data
- C. Reputation
- D. Customer lists

Answer: A

NEW QUESTION 470

- (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 472

- (Exam Topic 4)

Which of the following is the MOST effective way to identify an application backdoor prior to implementation?

- A. User acceptance testing (UAT)
- B. Database activity monitoring
- C. Source code review
- D. Vulnerability analysis

Answer: B

NEW QUESTION 477

- (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 482

- (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 487

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 490

- (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 494

- (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 495

- (Exam Topic 4)

A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?

- A. Prepare a business case for the response options.
- B. Identify resources for implementing responses.
- C. Develop a mechanism for monitoring residual risk.
- D. Update the risk register with the results.

Answer: D

NEW QUESTION 499

- (Exam Topic 4)

Which stakeholder is MOST important to include when defining a risk profile during the selection process for a new third party application'?

- A. The third-party risk manager
- B. The application vendor
- C. The business process owner
- D. The information security manager

Answer: B

NEW QUESTION 502

- (Exam Topic 4)

The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

- A. data logging and monitoring
- B. data mining and analytics
- C. data classification and labeling
- D. data retention and destruction

Answer: C

NEW QUESTION 505

- (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 506

- (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 509

- (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 511

- (Exam Topic 4)

Who is BEST suited to provide objective input when updating residual risk to reflect the results of control effectiveness?

- A. Control owner
- B. Risk owner
- C. Internal auditor
- D. Compliance manager

Answer: C

NEW QUESTION 513

- (Exam Topic 4)

Which of the following would BEST mitigate an identified risk scenario?

- A. Conducting awareness training
- B. Executing a risk response plan
- C. Establishing an organization's risk tolerance
- D. Performing periodic audits

Answer: C

NEW QUESTION 517

- (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 518

- (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 520

- (Exam Topic 4)

When developing risk scenario using a list of generic scenarios based on industry best practices, it is MOST imported 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 525

- (Exam Topic 4)

Which of the following BEST facilitates the identification of appropriate key performance indicators (KPIs) for a risk management program?

- A. Reviewing control objectives
- B. Aligning with industry best practices
- C. Consulting risk owners
- D. Evaluating KPIs in accordance with risk appetite

Answer: C

NEW QUESTION 528

- (Exam Topic 4)

Which of the following s MOST likely to deter an employee from engaging in inappropriate use of company owned IT systems?

- A. A centralized computer security response team
- B. Regular performance reviews and management check-ins
- C. Code of ethics training for all employees
- D. Communication of employee activity monitoring

Answer: D

NEW QUESTION 533

- (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 534

- (Exam Topic 4)

Which of the following is the BEST method to mitigate the risk of an unauthorized employee viewing confidential data in a database"

- A. Implement role-based access control
- B. Implement a data masking process
- C. Include sanctions in nondisclosure agreements (NDAs)
- D. Install a data loss prevention (DLP) tool

Answer: A

NEW QUESTION 539

- (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 544

- (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 546

- (Exam Topic 4)

Which of the following should be considered FIRST when creating a comprehensive IT risk register?

- A. Risk management budget
- B. Risk mitigation policies
- C. Risk appetite
- D. Risk analysis techniques

Answer: C

NEW QUESTION 550

- (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 551

- (Exam Topic 4)

Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

- A. The number of stakeholders involved in IT risk identification workshops
- B. The percentage of corporate budget allocated to IT risk activities
- C. The percentage of incidents presented to the board
- D. The number of executives attending IT security awareness training

Answer: B

NEW QUESTION 554

- (Exam Topic 4)

Which of the following is the GREATEST benefit of centralizing IT systems?

- A. Risk reporting
- B. Risk classification
- C. Risk monitoring
- D. Risk identification

Answer: C

NEW QUESTION 556

- (Exam Topic 4)

Which of the following is MOST important for successful incident response?

- A. The quantity of data logged by the attack control tools
- B. Blocking the attack route immediately
- C. The ability to trace the source of the attack
- D. The timeliness of attack recognition

Answer: D

NEW QUESTION 558

- (Exam Topic 4)

An organization is considering the adoption of an aggressive business strategy to achieve desired growth. From a risk management perspective, what should the risk practitioner do NEXT?

- A. Identify new threats resulting from the new business strategy
- B. Update risk awareness training to reflect current levels of risk appetite and tolerance
- C. Inform the board of potential risk scenarios associated with aggressive business strategies
- D. Increase the scale for measuring impact due to threat materialization

Answer: A

NEW QUESTION 561

- (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 564

- (Exam Topic 4)

Which of the following is the PRIMARY objective of maintaining an information asset inventory?

- A. To provide input to business impact analyses (BIAs)
- B. To protect information assets
- C. To facilitate risk assessments
- D. To manage information asset licensing

Answer: B

NEW QUESTION 568

- (Exam Topic 4)

In order to efficiently execute a risk response action plan, it is MOST important for the emergency response team members to understand:

- A. system architecture in target areas.
- B. IT management policies and procedures.
- C. business objectives of the organization.
- D. defined roles and responsibilities.

Answer: D

NEW QUESTION 573

- (Exam Topic 4)

A risk practitioner is reviewing accountability assignments for data risk in the risk register. Which of the following would pose the GREATEST concern?

- A. The risk owner is not the control owner for associated data controls.
- B. The risk owner is in a business unit and does not report through the IT department.
- C. The risk owner is listed as the department responsible for decision making.
- D. The risk owner is a staff member rather than a department manager.

Answer: C

NEW QUESTION 575

- (Exam Topic 4)

The cost of maintaining a control has grown to exceed the potential loss. Which of the following BEST describes this situation?

- A. Insufficient risk tolerance
- B. Optimized control management
- C. Effective risk management
- D. Over-controlled environment

Answer: B

NEW QUESTION 576

- (Exam Topic 4)

Which of the following is the BEST way to determine whether system settings are in alignment with control baselines?

- A. Configuration validation
- B. Control attestation
- C. Penetration testing
- D. Internal audit review

Answer: A

NEW QUESTION 581

- (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 585

- (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 589

- (Exam Topic 4)

Which of the following is the BEST way to protect sensitive data from administrators within a public cloud?

- A. Use an encrypted tunnel to connect to the cloud.
- B. Encrypt the data in the cloud database.
- C. Encrypt physical hard drives within the cloud.
- D. Encrypt data before it leaves the organization.

Answer: D

NEW QUESTION 591

- (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 594

- (Exam Topic 4)

Which of the following is the BEST course of action when an organization wants to reduce likelihood in order to reduce a risk level?

- A. Monitor risk controls.
- B. Implement preventive measures.
- C. Implement detective controls.
- D. Transfer the risk.

Answer: B

NEW QUESTION 596

- (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 597

- (Exam Topic 4)

An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

- A. Limited organizational knowledge of the underlying technology
- B. Lack of commercial software support
- C. Varying costs related to implementation and maintenance
- D. Slow adoption of the technology across the financial industry

Answer: A

NEW QUESTION 600

- (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 601

- (Exam Topic 4)

Which of the following is MOST important to include when reporting the effectiveness of risk management to senior management?

- A. Changes in the organization's risk appetite and risk tolerance levels
- B. Impact due to changes in external and internal risk factors
- C. Changes in residual risk levels against acceptable levels
- D. Gaps in best practices and implemented controls across the industry

Answer: C

NEW QUESTION 605

- (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 609

- (Exam Topic 4)

Which of the following is MOST important for senior management to review during an acquisition?

- A. Risk appetite and tolerance
- B. Risk framework and methodology
- C. Key risk indicator (KRI) thresholds
- D. Risk communication plan

Answer: A

NEW QUESTION 612

- (Exam Topic 4)

Which of the following is MOST important to update when an organization's risk appetite changes?

- A. Key risk indicators (KRIs)
- B. Risk reporting methodology
- C. Key performance indicators (KPIs)
- D. Risk taxonomy

Answer: A

NEW QUESTION 617

- (Exam Topic 4)

Which key performance efficiency (KPI) BEST measures the effectiveness of an organization's disaster recovery program?

- A. Number of service level agreement (SLA) violations
- B. Percentage of recovery issues identified during the exercise
- C. Number of total systems recovered within the recovery point objective (RPO)
- D. Percentage of critical systems recovered within the recovery time objective (RTO)

Answer: D

NEW QUESTION 620

- (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 621

- (Exam Topic 4)

What is the BEST recommendation to reduce the risk associated with potential system compromise when a vendor stops releasing security patches and updates for a business-critical legacy system?

- A. Segment the system on its own network.
- B. Ensure regular backups take place.
- C. Virtualize the system in the cloud.
- D. Install antivirus software on the system.

Answer: A

NEW QUESTION 623

- (Exam Topic 4)

Who is the BEST person to the employee personal data?

- A. Human resources (HR) manager
- B. System administrator
- C. Data privacy manager
- D. Compliance manager

Answer: A

NEW QUESTION 625

- (Exam Topic 4)

Of the following, who is responsible for approval when a change in an application system is ready for release to production?

- A. Information security officer
- B. IT risk manager
- C. Business owner
- D. Chief risk officer (CRO)

Answer: C

NEW QUESTION 629

- (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 632

- (Exam Topic 4)

An IT risk threat analysis is BEST used to establish

- A. risk scenarios
- B. risk maps
- C. risk appetite
- D. risk ownership.

Answer: A

NEW QUESTION 633

- (Exam Topic 4)

Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

- A. To identify gaps in data protection controls
- B. To develop a customer notification plan
- C. To identify personally identifiable information (PII)
- D. To determine gaps in data identification processes

Answer: A

NEW QUESTION 635

- (Exam Topic 4)

Which of the following is the GREATEST concern when establishing key risk indicators (KRIs)?

- A. High percentage of lagging indicators
- B. Nonexistent benchmark analysis
- C. Incomplete documentation for KRI monitoring
- D. Ineffective methods to assess risk

Answer: B

NEW QUESTION 637

- (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 639

- (Exam Topic 4)

Which of the following would be of GREATEST concern regarding an organization's asset management?

- A. Lack of a mature records management program
- B. Lack of a dedicated asset management team
- C. Decentralized asset lists
- D. Incomplete asset inventory

Answer: D

NEW QUESTION 640

- (Exam Topic 4)

Which of the following is MOST important to determine as a result of a risk assessment?

- A. Process ownership
- B. Risk appetite statement
- C. Risk tolerance levels
- D. Risk response options

Answer: D

NEW QUESTION 645

- (Exam Topic 4)

Which of the following is the GREATEST benefit of a three lines of defense structure?

- A. An effective risk culture that empowers employees to report risk
- B. Effective segregation of duties to prevent internal fraud
- C. Clear accountability for risk management processes
- D. Improved effectiveness and efficiency of business operations

Answer: C

NEW QUESTION 648

- (Exam Topic 4)

The MAIN purpose of selecting a risk response is to.

- A. ensure compliance with local regulatory requirements
- B. demonstrate the effectiveness of risk management practices.
- C. ensure organizational awareness of the risk level
- D. mitigate the residual risk to be within tolerance

Answer: C

NEW QUESTION 653

- (Exam Topic 4)

What should be the PRIMARY consideration related to data privacy protection when there are plans for a business initiative to make use of personal information?

- A. Do not collect or retain data that is not needed.
- B. Redact data where possible.
- C. Limit access to the personal data.
- D. Ensure all data is encrypted at rest and during transit.

Answer: D

NEW QUESTION 654

- (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 659

- (Exam Topic 4)

An organization recently implemented a machine learning-based solution to monitor IT usage and analyze user behavior in an effort to detect internal fraud. Which of the following is MOST likely to be reassessed as a result of this initiative?

- A. Risk likelihood
- B. Risk culture
- C. Risk appetite
- D. Risk capacity

Answer: A

NEW QUESTION 663

- (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 668

- (Exam Topic 4)

During a risk assessment, a risk practitioner learns that an IT risk factor is adequately mitigated by compensating controls in an associated business process. Which of the following would enable the MOST effective management of the residual risk?

- A. Schedule periodic reviews of the compensating controls' effectiveness.
- B. Report the use of compensating controls to senior management.
- C. Recommend additional IT controls to further reduce residual risk.
- D. Request that ownership of the compensating controls is reassigned to IT

Answer: A

NEW QUESTION 673

- (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 677

- (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 682

- (Exam Topic 4)

An internal audit report reveals that a legacy system is no longer supported Which of the following is the risk practitioner's MOST important action before recommending a risk response'

- A. Review historical application down me and frequency
- B. Assess the potential impact and cost of mitigation
- C. identify other legacy systems within the organization
- D. Explore the feasibility of replacing the legacy system

Answer: B

NEW QUESTION 686

- (Exam Topic 4)

The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.

Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading to data compromise	Risk Council	End-User Computing Manager AND Inventory	IT Operations Manager AND Security Operations Manager	Low Likelihood	Very Serious	0.120	Mitigate	Purchase and acquire data encryption software for mobile devices
R003	Fire Hazard	A fire accident may destroy data center equipment and servers leading to loss of availability and services	Information Security Department	Data Center Facilities Manager	Facilities Manager	Low Likelihood	Serious	0.060	Transfer	Buy fire hazard insurance policy
		A disgruntled								
		Significant				0.10	Low Likelihood			0.30
		Serious				0.20	Likely			0.50
		Very Serious				0.40	Highly Likely			0.70
		Catastrophic				0.80	Near Certainty			0.90

After implementing countermeasures listed in "Risk Response Descriptions" for each of the Risk IDs, which of the following component of the register MUST change?

- A. Risk Impact Rating
- B. Risk Owner
- C. Risk Likelihood Rating
- D. Risk Exposure

Answer: B

NEW QUESTION 691

- (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 696

- (Exam Topic 4)

It was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern?

- A. The underutilization of the replicated link
- B. The cost of recovering the data
- C. The lack of integrity of data
- D. The loss of data confidentiality

Answer: C

NEW QUESTION 701

- (Exam Topic 4)

Which of the following is a risk practitioner's BEST course of action after identifying risk scenarios related to noncompliance with new industry regulations?

- A. Escalate to senior management.
- B. Transfer the risk.
- C. Implement monitoring controls.
- D. Recalculate the risk.

Answer: D

NEW QUESTION 702

- (Exam Topic 3)

Which of the following will be the GREATEST concern when assessing the risk profile of an organization?

- A. The risk profile was not updated after a recent incident
- B. The risk profile was developed without using industry standards.
- C. The risk profile was last reviewed two years ago.
- D. The risk profile does not contain historical loss data.

Answer: A

NEW QUESTION 707

- (Exam Topic 3)

What information is MOST helpful to asset owners when classifying organizational assets for risk assessment?

- A. Potential loss to tie business due to non-performance of the asset
- B. Known emerging environmental threats
- C. Known vulnerabilities published by the asset developer
- D. Cost of replacing the asset with a new asset providing similar services

Answer: A

NEW QUESTION 712

- (Exam Topic 3)

Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

- A. Activity logging and monitoring
- B. Periodic access review
- C. Two-factor authentication
- D. Awareness training and background checks

Answer: A

NEW QUESTION 713

- (Exam Topic 3)

Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

- A. Senior management has approved the control design.
- B. Inherent risk has been reduced from original levels.
- C. Residual risk remains within acceptable levels.
- D. Costs for control maintenance are reasonable.

Answer: C

NEW QUESTION 715

- (Exam Topic 3)

A risk practitioner has just learned about new malware that has severely impacted industry peers worldwide data loss?

- A. Customer database manager
- B. Customer data custodian
- C. Data privacy officer
- D. Audit committee

Answer: B

NEW QUESTION 719

- (Exam Topic 3)

Upon learning that the number of failed back-up attempts continually exceeds the current risk threshold, the risk practitioner should:

- A. inquire about the status of any planned corrective actions
- B. keep monitoring the situation as there is evidence that this is normal
- C. adjust the risk threshold to better reflect actual performance
- D. initiate corrective action to address the known deficiency

Answer: D

NEW QUESTION 720

- (Exam Topic 3)

To minimize the risk of a potential acquisition being exposed externally, an organization has selected a few key employees to be engaged in the due diligence process. A member of the due diligence team realizes a close acquaintance is a high-ranking IT professional at a subsidiary of the company about to be acquired. What is the BEST course of action for this team member?

- A. Enforce segregation of duties.
- B. Disclose potential conflicts of interest.
- C. Delegate responsibilities involving the acquaintance.
- D. Notify the subsidiary's legal team.

Answer: B

NEW QUESTION 725

- (Exam Topic 3)

Which of the following BEST supports ethical IT risk management practices?

- A. Robust organizational communication channels
- B. Mapping of key risk indicators (KRIs) to corporate strategy
- C. Capability maturity models integrated with risk management frameworks
- D. Rigorously enforced operational service level agreements (SLAs)

Answer: A

NEW QUESTION 728

- (Exam Topic 3)

Which of the following would be MOST helpful to an information security management team when allocating resources to mitigate exposures?

- A. Relevant risk case studies
- B. Internal audit findings
- C. Risk assessment results
- D. Penetration testing results

Answer: C

NEW QUESTION 729

- (Exam Topic 3)

Which of the following would BEST mitigate the risk associated with reputational damage from inappropriate use of social media sites by employees?

- A. Validating employee social media accounts and passwords
- B. Monitoring Internet usage on employee workstations
- C. Disabling social media access from the organization's technology
- D. Implementing training and awareness programs

Answer: D

NEW QUESTION 733

- (Exam Topic 3)

A chief information officer (CIO) has identified risk associated with shadow systems being maintained by business units to address specific functionality gaps in the organization's enterprise resource planning (ERP) system. What is the BEST way to reduce this risk going forward?

- A. Align applications to business processes.
- B. Implement an enterprise architecture (EA).
- C. Define the software development life cycle (SDLC).
- D. Define enterprise-wide system procurement requirements.

Answer: B

NEW QUESTION 738

- (Exam Topic 3)

Which element of an organization's risk register is MOST important to update following the commissioning of a new financial reporting system?

- A. Key risk indicators (KRIs)
- B. The owner of the financial reporting process
- C. The risk rating of affected financial processes
- D. The list of relevant financial controls

Answer: C

NEW QUESTION 743

- (Exam Topic 3)

Which of the following is MOST important to communicate to senior management during the initial implementation of a risk management program?

- A. Regulatory compliance
- B. Risk ownership
- C. Best practices
- D. Desired risk level

Answer: D

NEW QUESTION 748

- (Exam Topic 3)

A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

- A. Ask the business to make a budget request to remediate the problem.
- B. Build a business case to remediate the fix.
- C. Research the types of attacks the threat can present.
- D. Determine the impact of the missing threat.

Answer: D

NEW QUESTION 750

- (Exam Topic 3)

Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

- A. Updating the risk register to include the risk mitigation plan
- B. Determining processes for monitoring the effectiveness of the controls
- C. Ensuring that control design reduces risk to an acceptable level
- D. Confirming to management the controls reduce the likelihood of the risk

Answer: C

NEW QUESTION 752

- (Exam Topic 3)

When developing a risk awareness training program, which of the following training topics would BEST facilitate a thorough understanding of risk scenarios?

- A. Mapping threats to organizational objectives
- B. Reviewing past audits
- C. Analyzing key risk indicators (KRIs)
- D. Identifying potential sources of risk

Answer: D

NEW QUESTION 754

- (Exam Topic 3)

What is the PRIMARY purpose of a business impact analysis (BIA)?

- A. To determine the likelihood and impact of threats to business operations
- B. To identify important business processes in the organization
- C. To estimate resource requirements for related business processes
- D. To evaluate the priority of business operations in case of disruption

Answer: D

NEW QUESTION 757

- (Exam Topic 3)

Who should be PRIMARILY responsible for establishing an organization's IT risk culture?

- A. Business process owner
- B. Executive management
- C. Risk management
- D. IT management

Answer: B

NEW QUESTION 761

- (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 765

- (Exam Topic 3)

Which of the following BEST informs decision-makers about the value of a notice and consent control for the collection of personal information?

- A. A comparison of the costs of notice and consent control options
- B. Examples of regulatory fines incurred by industry peers for noncompliance
- C. A report of critical controls showing the importance of notice and consent
- D. A cost-benefit analysis of the control versus probable legal action

Answer: D

NEW QUESTION 768

- (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 771

- (Exam Topic 3)

Prudent business practice requires that risk appetite not exceed:

- A. inherent risk.
- B. risk tolerance.
- C. risk capacity.
- D. residual risk.

Answer: C

NEW QUESTION 775

- (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 780

- (Exam Topic 3)

After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?

- A. Obtain industry benchmarks related to the specific risk.
- B. Provide justification for the lower risk rating.
- C. Notify the business at the next risk briefing.
- D. Reopen the risk issue and complete a full assessment.

Answer: B

NEW QUESTION 783

- (Exam Topic 3)

Senior management has asked a risk practitioner to develop technical risk scenarios related to a recently developed enterprise resource planning (ERP) system. These scenarios will be owned by the system manager. Which of the following would be the BEST method to use when developing the scenarios?

- A. Cause-and-effect diagram
- B. Delphi technique
- C. Bottom-up approach
- D. Top-down approach

Answer: A

NEW QUESTION 785

- (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 789

- (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 790

- (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 795

- (Exam Topic 3)

Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

- A. Occurrences of specific events
- B. A performance measurement
- C. The risk tolerance level
- D. Risk scenarios

Answer: C

NEW QUESTION 797

- (Exam Topic 3)

The acceptance of control costs that exceed risk exposure MOST likely demonstrates:

- A. corporate culture alignment
- B. low risk tolerance
- C. high risk tolerance
- D. corporate culture misalignment.

Answer: C

NEW QUESTION 800

- (Exam Topic 3)

The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

- A. accounts without documented approval
- B. user accounts with default passwords
- C. active accounts belonging to former personnel
- D. accounts with dormant activity.

Answer: A

NEW QUESTION 802

- (Exam Topic 3)

The MAIN purpose of reviewing a control after implementation is to validate that the control:

- A. operates as intended.
- B. is being monitored.
- C. meets regulatory requirements.
- D. operates efficiently.

Answer: A

NEW QUESTION 807

- (Exam Topic 3)

Which of the following is MOST important when developing risk scenarios?

- A. Reviewing business impact analysis (BIA)
- B. Collaborating with IT audit
- C. Conducting vulnerability assessments
- D. Obtaining input from key stakeholders

Answer: D

NEW QUESTION 811

- (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 815

- (Exam Topic 3)

Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?

- A. Develop a risk treatment plan.
- B. Validate organizational risk appetite.
- C. Review results of prior risk assessments.
- D. Include the current and desired states in the risk register.

Answer: A

NEW QUESTION 818

- (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 821

- (Exam Topic 3)

Which of the following will BEST help in communicating strategic risk priorities?

- A. Heat map
- B. Business impact analysis (BIA)
- C. Balanced Scorecard
- D. Risk register

Answer: A

NEW QUESTION 824

- (Exam Topic 3)

Which of the following is the PRIMARY reason to adopt key control indicators (KCIs) in the risk monitoring and reporting process?

- A. To provide data for establishing the risk profile
- B. To provide assurance of adherence to risk management policies
- C. To provide measurements on the potential for risk to occur
- D. To provide assessments of mitigation effectiveness

Answer: D

NEW QUESTION 828

- (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 833

- (Exam Topic 3)

Which of the following approaches would BEST help to identify relevant risk scenarios?

- A. Engage line management in risk assessment workshops.
- B. Escalate the situation to risk leadership.
- C. Engage internal audit for risk assessment workshops.
- D. Review system and process documentation.

Answer: A

NEW QUESTION 835

- (Exam Topic 3)

Which of the following should be done FIRST when information is no longer required to support business objectives?

- A. Archive the information to a backup database.
- B. Protect the information according to the classification policy.
- C. Assess the information against the retention policy.
- D. Securely and permanently erase the information

Answer: C

NEW QUESTION 837

- (Exam Topic 3)

Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?

- A. Unknown vulnerabilities
- B. Legacy technology systems
- C. Network isolation
- D. Overlapping threats

Answer: D

NEW QUESTION 838

- (Exam Topic 3)

The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

- A. assess gaps in IT risk management operations and strategic focus.
- B. confirm that IT risk assessment results are expressed as business impact.
- C. verify implemented controls to reduce the likelihood of threat materialization.
- D. ensure IT risk management is focused on mitigating potential risk.

Answer: D

NEW QUESTION 842

- (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 846

- (Exam Topic 3)

During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?

- A. Conduct a comprehensive review of access management processes.
- B. Declare a security incident and engage the incident response team.
- C. Conduct a comprehensive awareness session for system administrators.
- D. Evaluate system administrators' technical skills to identify if training is required.

Answer: A

NEW QUESTION 849

- (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 852

- (Exam Topic 3)

Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

- A. Complete an offsite business continuity exercise.
- B. Conduct a compliance check against standards.
- C. Perform a vulnerability assessment.
- D. Measure the change in inherent risk.

Answer: C

NEW QUESTION 855

- (Exam Topic 3)

An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

- A. Detective
- B. Directive
- C. Preventive
- D. Compensating

Answer: B

NEW QUESTION 859

- (Exam Topic 3)

An IT control gap has been identified in a key process. Who would be the MOST appropriate owner of the risk associated with this gap?

- A. Key control owner
- B. Operational risk manager
- C. Business process owner
- D. Chief information security officer (CISO)

Answer: A

NEW QUESTION 860

- (Exam Topic 3)

Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?

- A. Relevance to the business process
- B. Regulatory compliance requirements
- C. Cost-benefit analysis
- D. Comparison against best practice

Answer: B

NEW QUESTION 864

- (Exam Topic 3)

Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

- A. Aligning IT with short-term and long-term goals of the organization
- B. Ensuring the IT budget and resources focus on risk management
- C. Ensuring senior management's primary focus is on the impact of identified risk
- D. Prioritizing internal departments that provide service to customers

Answer: A

NEW QUESTION 866

- (Exam Topic 3)

When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction based on:

- A. cost-benefit analysis.
- B. risk appetite.
- C. regulatory guidelines
- D. control efficiency

Answer: A

NEW QUESTION 869

- (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 873

- (Exam Topic 3)

Which of the following MUST be updated to maintain an IT risk register?

- A. Expected frequency and potential impact
- B. Risk tolerance
- C. Enterprise-wide IT risk assessment
- D. Risk appetite

Answer: C

NEW QUESTION 874

- (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 877

- (Exam Topic 3)

While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially. Which of the following would be the BEST approach for the risk practitioner to take?

- A. Temporarily suspend emergency changes.
- B. Document the control deficiency in the risk register.
- C. Conduct a root cause analysis.
- D. Continue monitoring change management metrics.

Answer: C

NEW QUESTION 880

- (Exam Topic 3)

Which of the following would BEST help to address the risk associated with malicious outsiders modifying application data?

- A. Multi-factor authentication
- B. Role-based access controls
- C. Activation of control audits
- D. Acceptable use policies

Answer: A

NEW QUESTION 881

- (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 883

- (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 886

- (Exam Topic 2)

An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

- A. Review the risk identification process.
- B. Inform the risk scenario owners.
- C. Create a risk awareness communication plan.
- D. Update the risk register.

Answer: A

NEW QUESTION 889

- (Exam Topic 2)

A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner's FIRST course of action?

- A. Update the KRI threshold.
- B. Recommend additional controls.
- C. Review incident handling procedures.
- D. Perform a root cause analysis.

Answer: D

NEW QUESTION 892

- (Exam Topic 2)

The PRIMARY benefit of classifying information assets is that it helps to:

- A. communicate risk to senior management
- B. assign risk ownership
- C. facilitate internal audit
- D. determine the appropriate level of control

Answer: D

NEW QUESTION 895

- (Exam Topic 2)

When reviewing a risk response strategy, senior management's PRIMARY focus should be placed on the:

- A. cost-benefit analysis.
- B. investment portfolio.
- C. key performance indicators (KPIs).
- D. alignment with risk appetite.

Answer: D

NEW QUESTION 898

- (Exam Topic 2)

The purpose of requiring source code escrow in a contractual agreement is to:

- A. ensure that the source code is valid and exists.
- B. ensure that the source code is available if the vendor ceases to exist.
- C. review the source code for adequacy of controls.
- D. ensure the source code is available when bugs occur.

Answer: B

NEW QUESTION 903

- (Exam Topic 2)

Mapping open risk issues to an enterprise risk heat map BEST facilitates:

- A. risk response.
- B. control monitoring.
- C. risk identification.
- D. risk ownership.

Answer: A

NEW QUESTION 907

- (Exam Topic 2)

Controls should be defined during the design phase of system development because:

- A. it is more cost-effective to determine controls in the early design phase.
- B. structured analysis techniques exclude identification of controls.
- C. structured programming techniques require that controls be designed before coding begins.
- D. technical specifications are defined during this phase.

Answer: A

NEW QUESTION 911

.....

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](#)