Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (Exam Topic 4)
When developing a response plan to address security incidents regarding sensitive data loss, it is MOST important

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

Answer: C

NEW QUESTION 2
- (Exam Topic 4)
A global company s business continuity plan (BCP) requires the transfer of its customer information…. event of a disaster. Which of the following should be the MOST important risk consideration?

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

Answer: B

NEW QUESTION 3
- (Exam Topic 4)
A 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 4
- (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 5
- (Exam Topic 4)
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, 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 6
- (Exam Topic 4)
Which of the following would provide the MOST reliable evidence of the effectiveness of security controls implemented for a web application?

A. Penetration testing
B. IT general controls audit
C. Vulnerability assessment
D. Fault tree analysis

Answer: A

NEW QUESTION 7
- (Exam Topic 4)
The BEST metric to demonstrate that servers are configured securely is the total number of servers:

A. exceeding availability thresholds
B. experiencing hardware failures
C. exceeding current patching standards.

D. meeting the baseline for hardening.

Answer: D

NEW QUESTION 8
- (Exam Topic 4)
Using key risk indicators (KRIs) to illustrate changes in the risk profile PRIMARILY helps to:

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

Answer: A

NEW QUESTION 9
- (Exam Topic 4)
When a risk practitioner is determining a system's criticality. it is MOST helpful to review the associated:

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

Answer: B

NEW QUESTION 10
- (Exam Topic 4)
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 10
- (Exam Topic 4)
An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

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

Answer: B

NEW QUESTION 13
- (Exam Topic 4)
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

A. Several risk action plans have missed target completion dates.
B. Senior management has accepted more risk than usual.
C. Risk associated with many assets is only expressed in qualitative terms.
D. Many risk scenarios are owned by the same senior manager.

Answer: A

NEW QUESTION 15
- (Exam Topic 4)
An organization is considering outsourcing user administration controls tor a critical system. The potential vendor has offered to perform quarterly sett-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to me risk practitioner?

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

Answer: D

NEW QUESTION 17
- (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 20
- (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 22
- (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 23
- (Exam Topic 4)
After undertaking a risk assessment of a production system, the MOST appropriate action is fcr the risk manager to

A. recommend a program that minimizes the concerns of that production system.
B. inform the process owner of the concerns and propose measures to reduce them.
C. inform the IT manager of the concerns and propose measures to reduce them.
D. inform the development team of the concerns and together formulate risk reduction measures.

Answer: B

NEW QUESTION 26
- (Exam Topic 4)
Which of the following would provide the BEST evidence of an effective internal control environment/?

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

Answer: D

NEW QUESTION 29
- (Exam Topic 4)
Which of the following is the PRIMARY reason for a risk practitioner to review an organization's IT asset inventory?

A. To plan for the replacement of assets at the end of their life cycles
B. To assess requirements for reducing duplicate assets
C. To understand vulnerabilities associated with the use of the assets
D. To calculate mean time between failures (MTBF) for the assets

Answer: C

NEW QUESTION 32
- (Exam Topic 4)
Which of the following practices would be MOST effective in protecting personality identifiable information
(Ptl) from unauthorized access m a cloud environment?

A. Apply data classification policy
B. Utilize encryption with logical access controls
C. Require logical separation of company data
D. Obtain the right to audit

Answer: B

NEW QUESTION 36
- (Exam Topic 4)
An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis Which of the following is the MOST important control to ensure the privacy of customer information?

A. Nondisclosure agreements (NDAs)
B. Data anonymization
C. Data cleansing
D. Data encryption

Answer: C

NEW QUESTION 40
- (Exam Topic 4)
An organization has asked an IT risk practitioner to conduct an operational risk assessment on an initiative to outsource the organization's customer service operations overseas. Which of the following would MOST significantly impact management's decision?

A. Time zone difference of the outsourcing location
B. Ongoing financial viability of the outsourcing company
C. Cross-border information transfer restrictions in the outsourcing country
D. Historical network latency between the organization and outsourcing location

Answer: C

NEW QUESTION 42
- (Exam Topic 4)
Which of the following is MOST likely to introduce risk for financial institutions that use blockchain?

A. Cost of implementation
B. Implementation of unproven applications
C. Disruption to business processes
D. Increase in attack surface area

Answer: B

NEW QUESTION 47
- (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 48
- (Exam Topic 4)
Which of the following is the PRIMARY purpose of creating and documenting control procedures?

A. To facilitate ongoing audit and control testing
B. To help manage risk to acceptable tolerance levels
C. To establish and maintain a control inventory
D. To increase the likelihood of effective control operation

Answer: D

NEW QUESTION 50
- (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 identity all relevant issues.
B. be too costly
C. violate laws in other countries
D. be too line consuming

Answer: C

NEW QUESTION 53
- (Exam Topic 4)
Which of the following provides the BEST assurance of the effectiveness of vendor security controls?

A. Review vendor control self-assessments (CSA).
B. Review vendor service level agreement (SLA) metrics.
C. Require independent control assessments.
D. Obtain vendor references from existing customers.

Answer: C

NEW QUESTION 57
- (Exam Topic 3)
The PRIMARY reason for prioritizing risk scenarios is to:

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

Answer: D

NEW QUESTION 62
- (Exam Topic 4)
A risk practitioner implemented a process to notify management of emergency changes that may not be approved. Which of the following is the BEST way to provide this information to management?

A. Change logs
B. Change management meeting minutes
C. Key control indicators (KCIs)
D. Key risk indicators (KRIs)

Answer: C

NEW QUESTION 64
- (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 67
- (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 72
- (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 74
- (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 76
- (Exam Topic 4)
Which of the following BEST enables risk-based decision making in support of a business continuity plan (BCP)?

A. Impact analysis

B. Control analysis
C. Root cause analysis
D. Threat analysis

Answer: A

NEW QUESTION 78
- (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 81
- (Exam Topic 3)
An organization has implemented a preventive control to lock user accounts after three unsuccessful login attempts. This practice has been proven to be unproductive, and a change in the control threshold value has been recommended. Who should authorize changing this threshold?

A. Risk owner
B. IT security manager
C. IT system owner
D. Control owner

Answer: D

NEW QUESTION 83
- (Exam Topic 3)
Which of the following statements describes the relationship between key risk indicators (KRIs) and key control indicators (KCIs)?

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

Answer: A

NEW QUESTION 88
- (Exam Topic 3)
Which of the following is the MOST effective control to maintain the integrity of system configuration files?

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

Answer: D

NEW QUESTION 92
- (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 fallowing 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 95
- (Exam Topic 3)
Winch of the following can be concluded by analyzing the latest vulnerability report for the it infrastructure?

A. Likelihood of a threat
B. Impact of technology risk
C. Impact of operational risk
D. Control weakness

Answer: C

NEW QUESTION 97

- (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 100
- (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 101
- (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 103
- (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 108
- (Exam Topic 3)
An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

A. Potential increase in regulatory scrutiny
B. Potential system downtime
C. Potential theft of personal information
D. Potential legal risk

Answer: C

NEW QUESTION 112
- (Exam Topic 3)
Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

A. Key performance indicators (KPIs)
B. Risk heat maps
C. Internal audit findings
D. Periodic penetration testing

Answer: A

NEW QUESTION 115
- (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 119
- (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 121
- (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 125
- (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 128
- (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 133
- (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 135
- (Exam Topic 3)
Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

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

Answer: B

NEW QUESTION 138
- (Exam Topic 3)
Risk acceptance of an exception to a security control would MOST likely be justified when:

A. automation cannot be applied to the control
B. business benefits exceed the loss exposure.

C. the end-user license agreement has expired.
D. the control is difficult to enforce in practice.

Answer: B

NEW QUESTION 142
- (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 144
- (Exam Topic 3)
Which of the following should be the PRIMARY goal of developing information security metrics?

A. Raising security awareness
B. Enabling continuous improvement
C. Identifying security threats
D. Ensuring regulatory compliance

Answer: B

NEW QUESTION 147
- (Exam Topic 3)
An organization has been notified that a disgruntled, terminated IT administrator has tried to break into the corporate network. Which of the following discoveries should be of GREATEST concern to the organization?

A. Authentication logs have been disabled.
B. An external vulnerability scan has been detected.
C. A brute force attack has been detected.
D. An increase in support requests has been observed.

Answer: A

NEW QUESTION 152
- (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 155
- (Exam Topic 3)
While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

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

Answer: B

NEW QUESTION 159
- (Exam Topic 3)
When of the following is the MOST significant exposure when an application uses individual user accounts to access the underlying database?

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

Answer: C

NEW QUESTION 164

- (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 167
- (Exam Topic 3)
A risk practitioner has been asked to advise management on developing a log collection and correlation strategy. Which of the following should be the MOST important consideration when developing this strategy?

A. Ensuring time synchronization of log sources.
B. Ensuring the inclusion of external threat intelligence log sources.
C. Ensuring the inclusion of all computing resources as log sources.
D. Ensuring read-write access to all log sources

Answer: A

NEW QUESTION 169
- (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 170
- (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 171
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for risk related to IT infrastructure failure?

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

Answer: B

NEW QUESTION 173
- (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 177
- (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 178
- (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 182
- (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 187
- (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 190
- (Exam Topic 3)
Which of the following will BEST support management reporting on risk?

A. Control self-assessment (CSA)
B. Risk policy requirements
C. A risk register
D. Key performance indicators (KPIs)

Answer: C

NEW QUESTION 194
- (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 198
- (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 200
- (Exam Topic 3)
A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

A. IT system owner
B. Chief financial officer
C. Chief risk officer
D. Business process owner

Answer: D

NEW QUESTION 205
- (Exam Topic 3)
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

A. obtain the support of executive management.
B. map the business processes to supporting IT and other corporate resources.
C. identify critical business processes and the degree of reliance on support services.
D. document the disaster recovery process.

Answer: C

NEW QUESTION 210
- (Exam Topic 3)
When of the following 15 MOST important when developing a business case for a proposed security investment?

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

Answer: B

NEW QUESTION 215
- (Exam Topic 3)
A risk practitioner is preparing a report to communicate changes in the risk and control environment. The BEST way to engage stakeholder attention is to:

A. include detailed deviations from industry benchmarks,
B. include a summary linking information to stakeholder needs,
C. include a roadmap to achieve operational excellence,
D. publish the report on-demand for stakeholders.

Answer: B

NEW QUESTION 220
- (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 223
- (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 228
- (Exam Topic 3)
Which of the following would be MOST helpful to a risk practitioner when ensuring that mitigated risk remains within acceptable limits?

A. Building an organizational risk profile after updating the risk register
B. Ensuring risk owners participate in a periodic control testing process
C. Designing a process for risk owners to periodically review identified risk
D. Implementing a process for ongoing monitoring of control effectiveness

Answer: D

NEW QUESTION 231
- (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 233
- (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 235
- (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 236
- (Exam Topic 3)
Which of the following is the GREATEST benefit for an organization with a strong risk awareness culture?

A. Reducing the involvement by senior management
B. Using more risk specialists
C. Reducing the need for risk policies and guidelines
D. Discussing and managing risk as a team

Answer: D

NEW QUESTION 241
- (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 242
- (Exam Topic 3)
Which of the following is necessary to enable an IT risk register to be consolidated with the rest of the organization’s risk register?

A. Risk taxonomy
B. Risk response
C. Risk appetite
D. Risk ranking

Answer: A

NEW QUESTION 244
- (Exam Topic 3)
Which of the following is the MOST important consideration for protecting data assets m a Business application system?

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

Answer: A

NEW QUESTION 248
- (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 250
- (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 255
- (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 256
- (Exam Topic 3)
An organization moved its payroll system to a Software as a Service (SaaS) application. A new data privacy regulation stipulates that data can only be processed within the country where it is collected. Which of the following should be done FIRST when addressing this situation?

A. Analyze data protection methods.
B. Understand data flows.
C. Include a right-to-audit clause.
D. Implement strong access controls.

Answer: B

NEW QUESTION 261
- (Exam Topic 3)
Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

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

Answer: D

NEW QUESTION 264
- (Exam Topic 3)
Which of the following data would be used when performing a business impact analysis (BIA)?

A. Cost-benefit analysis of running the current business
B. Cost of regulatory compliance
C. Projected impact of current business on future business
D. Expected costs for recovering the business

Answer: D

NEW QUESTION 267
- (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 269
- (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 274
- (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 277
- (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 281
- (Exam Topic 3)
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

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

Answer: A

NEW QUESTION 283
- (Exam Topic 3)
Which of the following is MOST important to compare against the corporate risk profile?

A. Industry benchmarks
B. Risk tolerance
C. Risk appetite
D. Regulatory compliance

Answer: D

NEW QUESTION 286
- (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 288
- (Exam Topic 3)
Analyzing trends in key control indicators (KCIs) BEST enables a risk practitioner to proactively identify impacts on an organization's:

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

Answer: C

NEW QUESTION 292

- (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 297
- (Exam Topic 3)
When formulating a social media policy lo 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 298
- (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 301
- (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 306
- (Exam Topic 3)
Which of the following controls BEST enables an organization to ensure a complete and accurate IT asset inventory?

A. Prohibiting the use of personal devices for business
B. Performing network scanning for unknown devices
C. Requesting an asset list from business owners
D. Documenting asset configuration baselines

Answer: B

NEW QUESTION 309
- (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 311
- (Exam Topic 3)
Which of the following methods is an example of risk mitigation?

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

Answer: C

NEW QUESTION 312
- (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 317
- (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 318
- (Exam Topic 3)
Which of the following is the BEST source for identifying key control indicators (KCIs)?

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

Answer: B

NEW QUESTION 322
- (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 325
- (Exam Topic 3)
Who is BEST suited to determine whether a new control properly mitigates data loss risk within a system?

A. Data owner
B. Control owner
C. Risk owner
D. System owner

Answer: B

NEW QUESTION 330
- (Exam Topic 3)
Which of We 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 prowler 10 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 332
- (Exam Topic 3)
Print jobs containing confidential information are sent to a shared network printer located in a secure room. Which of the following is the BEST control to prevent the inappropriate disclosure of confidential information?

A. Requiring a printer access code for each user
B. Using physical controls to access the printer room
C. Using video surveillance in the printer room
D. Ensuring printer parameters are properly configured

Answer:

A

NEW QUESTION 335
- (Exam Topic 3)
Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?

A. The value at which control effectiveness would fail
B. Thresholds benchmarked to peer organizations
C. A typical operational value
D. A value that represents the intended control state

Answer: A

NEW QUESTION 340
- (Exam Topic 3)
An organization is implementing internet of Things (loT) technology to control temperature and lighting in its headquarters. Which of the following should be of GREATEST concern?

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

Answer: D

NEW QUESTION 342
- (Exam Topic 4)
Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

A. Board of directors
B. Vendors
C. Regulators
D. Legal team

Answer: A

NEW QUESTION 345
- (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 348
- (Exam Topic 4)
Which of the following is MOST important to ensure when reviewing an organization's risk register?

A. Risk ownership is recorded.
B. Vulnerabilities have separate entries.
C. Control ownership is recorded.
D. Residual risk is less than inherent risk.

Answer: A

NEW QUESTION 353
- (Exam Topic 4)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

A. Prioritize risk response options
B. Reduce likelihood.
C. Address more than one risk response
D. Reduce impact

Answer: C

NEW QUESTION 354
- (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 355
- (Exam Topic 4)
Recovery the objectives (RTOs) should be based on

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

Answer: C

NEW QUESTION 356
- (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 357
- (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 358
- (Exam Topic 4)
Which of the following is MOST helpful in defining an early-warning threshold associated with insufficient network bandwidth''

A. Average bandwidth usage
B. Peak bandwidth usage
C. Total bandwidth usage
D. Bandwidth used during business hours

Answer: A

NEW QUESTION 359
- (Exam Topic 4)
An information security audit identified a risk resulting from the failure of an automated control Who is responsible for ensuring the risk register is updated accordingly?

A. The risk practitioner
B. The risk owner
C. The control owner
D. The audit manager

Answer: A

NEW QUESTION 361
- (Exam Topic 4)
An organization has an approved bring your own device (BYOD) policy. Which of the following would BEST mitigate the security risk associated with the inappropriate use of enterprise applications on the devices?

A. Periodically review application on BYOD devices
B. Include BYOD in organizational awareness programs
C. Implement BYOD mobile device management (MDM) controls.
D. Enable a remote wee capability for BYOD devices

Answer: C

NEW QUESTION 366
- (Exam Topic 4)

Which risk response strategy could management apply to both positive and negative risk that has been identified?

A. Transfer
B. Accept
C. Exploit
D. Mitigate

Answer: B

NEW QUESTION 368
- (Exam Topic 4)
Which of the following would BEST facilitate the implementation of data classification requirements?

A. Implementing a data toss prevention (DLP) solution
B. Assigning a data owner
C. Scheduling periodic audits
D. Implementing technical controls over the assets

Answer: B

NEW QUESTION 369
- (Exam Topic 4)
Which of the following has the GREATEST influence on an organization's risk appetite?

A. Threats and vulnerabilities
B. Internal and external risk factors
C. Business objectives and strategies
D. Management culture and behavior

Answer: D

NEW QUESTION 370
- (Exam Topic 4)
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

A. KRIs assist in the preparation of the organization's risk profile.
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 provide an early warning that a risk threshold is about to be reached.

Answer: D

NEW QUESTION 371
- (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 374
- (Exam Topic 4)
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

A. Removing entries from the register after the risk has been treated
B. Recording and tracking the status of risk response plans within the register
C. Communicating the register to key stakeholders
D. Performing regular reviews and updates to the register

Answer: D

NEW QUESTION 376
- (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 377
- (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 382
- (Exam Topic 4)
Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

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

Answer: A

NEW QUESTION 384
- (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 actin 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 389
- (Exam Topic 4)
The PRIMARY objective of collecting information and reviewing documentation when performing periodic risk analysis should be to:

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

Answer: D

NEW QUESTION 390
- (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 395
- (Exam Topic 4)
Which of the following is the MOST effective way 10 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 400
- (Exam Topic 4)
The MAIN reason for prioritizing IT risk responses is to enable an organization to:

A. determine the risk appetite.
B. determine the budget.
C. define key performance indicators (KPIs).
D. optimize resource utilization.

Answer: C

NEW QUESTION 402
- (Exam Topic 4)
An organization's chief information officer (CIO) has proposed investing in a new. untested technology to take advantage of being first to market Senior management has concerns about the success of the project and has set a limit for expenditures before final approval. This conditional approval indicates the organization's risk:

A. capacity.
B. appetite.
C. management capability.
D. treatment strategy.

Answer: B

NEW QUESTION 405
- (Exam Topic 4)
Which of the following contributes MOST to the effective implementation of risk responses?

A. Clear understanding of the risk
B. Comparable industry risk trends
C. Appropriate resources
D. Detailed standards and procedures

Answer: A

NEW QUESTION 409
- (Exam Topic 4)
As pan of business continuity planning, which of the following is MOST important to include m a business impact analysis (BlA)?

A. An assessment of threats to the organization
B. An assessment of recovery scenarios
C. industry standard framework
D. Documentation of testing procedures

Answer: A

NEW QUESTION 413
- (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 arc 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 415
- (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 417
- (Exam Topic 4)
Which of the following is the PRIMARY objective of risk management?

A. Identify and analyze risk.
B. Achieve business objectives
C. Minimi2e business disruptions.
D. Identify threats and vulnerabilities.

Answer: B

NEW QUESTION 422
- (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? r

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 424
- (Exam Topic 4)
Who is MOST important lo include in the assessment of existing IT risk scenarios?

A. Technology subject matter experts
B. Business process owners
C. Business users of IT systems
D. Risk management consultants

Answer: C

NEW QUESTION 429
- (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 433
- (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 437
- (Exam Topic 4)
Which of the following is the PRIMARY reason for an organization to include an acceptable use banner when users log in?

A. To reduce the likelihood of insider threat
B. To eliminate the possibility of insider threat
C. To enable rapid discovery of insider threat
D. To reduce the impact of insider threat

Answer: A

NEW QUESTION 441
- (Exam Topic 4)
Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

A. Accountability may not be clearly defined.
B. Risk ratings may be inconsistently applied.
C. Different risk taxonomies may be used.
D. Mitigation efforts may be duplicated.

Answer: A

NEW QUESTION 443
- (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 446

- (Exam Topic 4)
Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

A. Service level agreements (SLAs) have not been met over the last quarter.
B. The service contract is up for renewal in less than thirty days.
C. Key third-party personnel have recently been replaced.
D. Monthly service charges are significantly higher than industry norms.

Answer: C

NEW QUESTION 451
- (Exam Topic 4)
An organization wants to launch a campaign to advertise a new product Using data analytics, the campaign can be targeted to reach potential customers. Which of the following should be of GREATEST concern to the risk practitioner?

A. Data minimization
B. Accountability
C. Accuracy
D. Purpose limitation

Answer: D

NEW QUESTION 456
- (Exam Topic 4)
Which of the following is the MOST important outcome of a business impact analysis (BIA)?

A. Understanding and prioritization of critical processes
B. Completion of the business continuity plan (BCP)
C. Identification of regulatory consequences
D. Reduction of security and business continuity threats

Answer: A

NEW QUESTION 459
- (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 461
- (Exam Topic 4)
Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

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

Answer: A

NEW QUESTION 464
- (Exam Topic 4)
An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

A. Identify the regulatory bodies that may highlight this gap
B. Highlight news articles about data breaches
C. Evaluate the risk as a measure of probable loss
D. Verify if competitors comply with a similar policy

Answer: B

NEW QUESTION 467
- (Exam Topic 4)
Which of the following is the PRIMARY reason to engage business unit managers in risk management processes'?

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

Answer: C

NEW QUESTION 470
- (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 473
- (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 478
- (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 482
- (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 483
- (Exam Topic 4)
A control process has been implemented in response to a new regulatory requirement, but has significantly reduced productivity. Which of the following is the BEST way to resolve this concern?

A. Absorb the loss in productivity.
B. Request a waiver to the requirements.
C. Escalate the issue to senior management
D. Remove the control to accommodate business objectives.

Answer: C

NEW QUESTION 484
- (Exam Topic 4)
An organization plans to implement a new Software as a Service (SaaS) speech-to-text solution Which of the following is MOST important to mitigate risk associated with data privacy?

A. Secure encryption protocols are utilized.
B. Multi-factor authentication is set up for users.
C. The solution architecture is approved by IT.
D. A risk transfer clause is included in the contact

Answer: A

NEW QUESTION 487
- (Exam Topic 4)
An organization has experienced a cyber attack that exposed customer personally identifiable information (Pll) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

A. Security control owners based on control failures
B. Cyber risk remediation plan owners
C. Risk owners based on risk impact

D. Enterprise risk management (ERM) team

Answer: C

NEW QUESTION 489
- (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 493
- (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 494
- (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 499
- (Exam Topic 4)
The MAJOR reason to classify information assets is

A. maintain a current inventory and catalog of information assets
B. determine their sensitivity and critical
C. establish recovery time objectives (RTOs)
D. categorize data into groups

Answer: C

NEW QUESTION 500
- (Exam Topic 4)
An organization has been experiencing an increasing number of spear phishing attacks Which of the following would be the MOST effective way to mitigate the risk associated with these attacks?

A. Update firewall configuration
B. Require strong password complexity
C. implement a security awareness program
D. Implement two-factor authentication

Answer: A

NEW QUESTION 504
- (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 505
- (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 509
- (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 514
- (Exam Topic 4)
Which of the following BEST reduces the risk associated with the theft of a laptop containing sensitive information?

A. Cable lock
B. Data encryption
C. Periodic backup
D. Biometrics access control

Answer: B

NEW QUESTION 517
- (Exam Topic 4)
Which of the following is MOST helpful in providing a high-level overview of current IT risk severity*?

A. Risk mitigation plans
B. heat map
C. Risk appetite statement
D. Key risk indicators (KRIs)

Answer: B

NEW QUESTION 518
- (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 lo 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 519
- (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 522
- (Exam Topic 4)
Which of the following is a risk practitioner's BEST recommendation upon learning that an employee inadvertently disclosed sensitive data to a vendor?

A. Enroll the employee in additional security training.
B. Invoke the incident response plan.
C. Conduct an internal audit.
D. Instruct the vendor to delete the data.

Answer: B

NEW QUESTION 523
- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 524
- (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 529
- (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 534
- (Exam Topic 4)
Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

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

Answer: B

NEW QUESTION 535
- (Exam Topic 4)
After an annual risk assessment is completed, which of the following would be MOST important to communicate to stakeholders?

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

Answer: B

NEW QUESTION 540
- (Exam Topic 4)
Which of the following would be the GREATEST concern for an IT risk practitioner when an employees.....

A. The organization's structure has not been updated
B. Unnecessary access permissions have not been removed.
C. Company equipment has not been retained by IT
D. Job knowledge was not transferred to employees m the former department

Answer: B

NEW QUESTION 545
- (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 ot 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 546
- (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 547
- (Exam Topic 4)
Which of the following is the MOST important step to ensure regulatory requirements are adequately addressed within an organization?

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

Answer: B

NEW QUESTION 550
- (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 554
- (Exam Topic 4)
Which of the following is the GREATEST benefit of identifying appropriate risk owners?

A. Accountability is established for risk treatment decisions
B. Stakeholders are consulted about risk treatment options
C. Risk owners are informed of risk treatment options
D. Responsibility is established for risk treatment decisions.

Answer: A

NEW QUESTION 558
- (Exam Topic 4)
When evaluating a number of potential controls for treating risk, it is MOST important to consider:

A. risk appetite and control efficiency.
B. inherent risk and control effectiveness.
C. residual risk and cost of control.
D. risk tolerance and control complexity.

Answer: C

NEW QUESTION 563
- (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 564
- (Exam Topic 4)
Which of the following should be the PRIMARY input to determine risk tolerance?

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

Answer: C

NEW QUESTION 566
- (Exam Topic 4)
Which of the following should be a risk practitioner's NEXT step after learning of an incident that has affected a competitor?

A. Activate the incident response plan.
B. Implement compensating controls.
C. Update the risk register.
D. Develop risk scenarios.

Answer: A

NEW QUESTION 569
- (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 574
- (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 577
- (Exam Topic 4)
Which of the following should be the PRIMARY basis for prioritizing risk responses?

A. The impact of the risk
B. The replacement cost of the business asset
C. The cost of risk mitigation controls
D. The classification of the business asset

Answer: A

NEW QUESTION 579
- (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 581
- (Exam Topic 4)
Which of the following is MOST important when determining risk appetite?

A. Assessing regulatory requirements
B. Benchmarking against industry standards
C. Gaining management consensus
D. Identifying risk tolerance

Answer: C

NEW QUESTION 586
- (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 591
- (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 594
- (Exam Topic 3)
Which of the following BEST indicates that an organization has implemented IT performance requirements?

A. Service level agreements (SLA)
B. Vendor references
C. Benchmarking data
D. Accountability matrix

Answer: A

NEW QUESTION 597
- (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 600
- (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 604
- (Exam Topic 3)
Which of the following describes the relationship between Key risk indicators (KRIs) and key control indicators (KCIS)?

A. KCIs are independent from KRIs KRIs.
B. KCIs and KRIs help in determining risk appetite.
C. KCIs are defined using data from KRIs.
D. KCIs provide input for KRIs

Answer: D

NEW QUESTION 606
- (Exam Topic 3)
When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

A. An analysis of the security logs that illustrate the sequence of events
B. An analysis of the impact of similar attacks in other organizations
C. A business case for implementing stronger logical access controls
D. A justification of corrective action taken

Answer: B

NEW QUESTION 610
- (Exam Topic 3)
When an organization’s disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?

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

Answer: B

NEW QUESTION 611
- (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 616
- (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 617
- (Exam Topic 3)
Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

A. Cost of controls
B. Risk tolerance
C. Risk appetite
D. Probability definition

Answer: A

NEW QUESTION 622
- (Exam Topic 3)
Which of the following BEST indicates that additional or improved controls ate needed m the environment?

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

Answer: D

NEW QUESTION 627
- (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 629
- (Exam Topic 3)
An organization planning to transfer and store its customer data with an offshore cloud service provider should be PRIMARILY concerned with:

A. data aggregation
B. data privacy
C. data quality
D. data validation

Answer: B

NEW QUESTION 632

- (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 637
- (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 639
- (Exam Topic 3)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

A. Relevance
B. Annual review
C. Automation
D. Management approval

Answer: A

NEW QUESTION 640
- (Exam Topic 3)
Of the following, who is accountable for ensuing the effectiveness of a control to mitigate risk?

A. Control owner
B. Risk manager
C. Control operator
D. Risk treatment owner

Answer: A

NEW QUESTION 643
- (Exam Topic 3)
Which of the following is the FIRST step in risk assessment?

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

Answer: B

NEW QUESTION 646
- (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 649
- (Exam Topic 3)
An organization's IT infrastructure is running end-of-life software that is not allowed without exception approval. Which of the following would provide the MOST helpful information to justify investing in updated software?

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

Answer: B

NEW QUESTION 651
- (Exam Topic 3)
Which of the following is the BEST course of action to help reduce the probability of an incident recurring?

A. Perform a risk assessment.
B. Perform root cause analysis.
C. Initiate disciplinary action.
D. Update the incident response plan.

Answer: B

NEW QUESTION 652
- (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 656
- (Exam Topic 3)
The PRIMARY purpose of IT control status reporting is to:

A. ensure compliance with IT governance strategy.
B. assist internal audit in evaluating and initiating remediation efforts.
C. benchmark IT controls with Industry standards.
D. facilitate the comparison of the current and desired states.

Answer: A

NEW QUESTION 659
- (Exam Topic 3)
Which of the following is the BEST indicator of an effective IT security awareness program?

A. Decreased success rate of internal phishing tests
B. Decreased number of reported security incidents
C. Number of disciplinary actions issued for security violations
D. Number of employees that complete security training

Answer: A

NEW QUESTION 661
- (Exam Topic 3)
An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?

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

Answer: C

NEW QUESTION 664
- (Exam Topic 3)
The BEST indication that risk management is effective is when risk has been reduced to meet:

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

Answer: C

NEW QUESTION 667
- (Exam Topic 3)
Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

A. Improved senior management communication
B. Optimized risk treatment decisions
C. Enhanced awareness of risk management
D. Improved collaboration among risk professionals

Answer:

B

NEW QUESTION 671
- (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 676
- (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 680
- (Exam Topic 3)
Which of the following BEST indicates the efficiency of a process for granting access privileges?

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

Answer: C

NEW QUESTION 685
- (Exam Topic 3)
A maturity model is MOST useful to an organization when it:

A. benchmarks against other organizations
B. defines a qualitative measure of risk
C. provides a reference for progress
D. provides risk metrics.

Answer: C

NEW QUESTION 688
- (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 690
- (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 691
- (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 695
- (Exam Topic 3)
Which of the following is the BEST way for an organization to enable risk treatment decisions?

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

Answer: C

NEW QUESTION 699
- (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 701
- (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 706
- (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 711
- (Exam Topic 3)
Which of the following would be a risk practitioner'$ BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

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

Answer: B

NEW QUESTION 715
- (Exam Topic 3)
Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:

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

Answer: B

NEW QUESTION 717
- (Exam Topic 3)
The MOST important consideration when selecting a control to mitigate an identified risk is whether:

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

Answer: A

NEW QUESTION 721
- (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 724
- (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 729
- (Exam Topic 3)
Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?

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

Answer: D

NEW QUESTION 734
- (Exam Topic 3)
An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

A. Implement database activity and capacity monitoring.
B. Ensure the business is aware of the risk.
C. Ensure the enterprise has a process to detect such situations.
D. Consider providing additional system resources to this job.

Answer: C

NEW QUESTION 737
- (Exam Topic 2)
Which of the following is MOST important for an organization that wants to reduce IT operational risk?

A. Increasing senior management's understanding of IT operations
B. Increasing the frequency of data backups
C. Minimizing complexity of IT infrastructure
D. Decentralizing IT infrastructure

Answer: C

NEW QUESTION 741
- (Exam Topic 2)
Which of the following risk scenarios would be the GREATEST concern as a result of a single sign-on implementation?

A. User access may be restricted by additional security.
B. Unauthorized access may be gained to multiple systems.
C. Security administration may become more complex.
D. User privilege changes may not be recorded.

Answer: B

NEW QUESTION 742

- (Exam Topic 2)
The PRIMARY objective of The board of directors periodically reviewing the risk profile is to help ensure:

A. the risk strategy is appropriate
B. KRIs and KPIs are aligned
C. performance of controls is adequate
D. the risk monitoring process has been established

Answer: A

NEW QUESTION 745
- (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 747
- (Exam Topic 2)
Quantifying the value of a single asset helps the organization to understand the:

A. overall effectiveness of risk management
B. consequences of risk materializing
C. necessity of developing a risk strategy,
D. organization s risk threshold.

Answer: B

NEW QUESTION 751
- (Exam Topic 2)
An organization is making significant changes to an application. At what point should the application risk profile be updated?

A. After user acceptance testing (UAT)
B. Upon release to production
C. During backlog scheduling
D. When reviewing functional requirements

Answer: D

NEW QUESTION 756
- (Exam Topic 2)
IT disaster recovery point objectives (RPOs) should be based on the:

A. maximum tolerable downtime.
B. maximum tolerable loss of data.
C. need of each business unit.
D. type of business.

Answer: C

NEW QUESTION 758
- (Exam Topic 2)
Which of the following is MOST commonly compared against the risk appetite?

A. IT risk
B. Inherent risk
C. Financial risk
D. Residual risk

Answer: D

NEW QUESTION 759
- (Exam Topic 2)
During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

A. Include the new risk scenario in the current risk assessment.
B. Postpone the risk assessment until controls are identified.
C. Request the risk scenario be removed from the register.
D. Exclude the new risk scenario from the current risk assessment

Answer: A

NEW QUESTION 762
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an anti-virus program?

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

Answer: C

NEW QUESTION 764
- (Exam Topic 2)
Which of the following could BEST detect an in-house developer inserting malicious functions into a web-based application?

A. Segregation of duties
B. Code review
C. Change management
D. Audit modules

Answer: B

NEW QUESTION 767
- (Exam Topic 2)
When assessing the maturity level of an organization's risk management framework, which of the following deficiencies should be of GREATEST concern to a risk practitioner?

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

Answer: C

NEW QUESTION 772
- (Exam Topic 2)
After identifying new risk events during a project, the project manager s NEXT step should be to:

A. determine if the scenarios need 10 be accepted or responded to.
B. record the scenarios into the risk register.
C. continue with a qualitative risk analysis.
D. continue with a quantitative risk analysis.

Answer: B

NEW QUESTION 773
- (Exam Topic 2)
Which of the following is a KEY outcome of risk ownership?

A. Risk responsibilities are addressed.
B. Risk-related information is communicated.
C. Risk-oriented tasks are defined.
D. Business process risk is analyzed.

Answer: A

NEW QUESTION 777
- (Exam Topic 2)
Which of the following statements in an organization's current risk profile report is cause for further action by senior management?

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

Answer: B

NEW QUESTION 778
- (Exam Topic 2)
Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?

A. Enhance the security awareness program.
B. Increase the frequency of incident reporting.
C. Purchase cyber insurance from a third party.
D. Conduct a control assessment.

Answer:

D

NEW QUESTION 782
- (Exam Topic 2)
Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?

A. Facilitating risk-aware decision making by stakeholders
B. Demonstrating management commitment to mitigate risk
C. Closing audit findings on a timely basis
D. Ensuring compliance to industry standards

Answer: A

NEW QUESTION 787
- (Exam Topic 2)
The PRIMARY purpose of a maturity model is to compare the:

A. current state of key processes to their desired state.
B. actual KPIs with target KPIs.
C. organization to industry best practices.
D. organization to peers.

Answer: A

NEW QUESTION 792
- (Exam Topic 2)
What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

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

Answer: B

NEW QUESTION 795
- (Exam Topic 2)
Due to a change in business processes, an identified risk scenario no longer requires mitigation. Which of the following is the MOST important reason the risk should remain in the risk register?

A. To support regulatory requirements
B. To prevent the risk scenario in the current environment
C. To monitor for potential changes to the risk scenario
D. To track historical risk assessment results

Answer: C

NEW QUESTION 799
- (Exam Topic 2)
Which of the following is the GREATEST risk associated with the use of data analytics?

A. Distributed data sources
B. Manual data extraction
C. Incorrect data selection
D. Excessive data volume

Answer: C

NEW QUESTION 804
- (Exam Topic 2)
An organization is considering modifying its system to enable acceptance of credit card payments. To reduce the risk of data exposure, which of the following should the organization do FIRST?

A. Conduct a risk assessment.
B. Update the security strategy.
C. Implement additional controls.
D. Update the risk register.

Answer: A

NEW QUESTION 806
- (Exam Topic 2)
Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

A. Key risk indicators (KRIs)
B. Data backups

C. Incident response plan
D. Cyber insurance

Answer: C

NEW QUESTION 810
- (Exam Topic 2)
An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

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

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

Answer: A

NEW QUESTION 814
- (Exam Topic 2)
Deviation from a mitigation action plan's completion date should be determined by which of the following?

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

Answer: D

NEW QUESTION 817
- (Exam Topic 2)
An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

A. External resources may need to be involved.
B. Data privacy regulations may be violated.
C. Recovery costs may increase significantly.
D. Service interruptions may be longer than anticipated.

Answer: D

NEW QUESTION 818
- (Exam Topic 2)
A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

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

Answer: A

NEW QUESTION 819
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to ensure once a risk action plan has been completed?

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

Answer: B

NEW QUESTION 821
- (Exam Topic 2)
Which of the following BEST helps to balance the costs and benefits of managing IT risk?

A. Prioritizing risk responses
B. Evaluating risk based on frequency and probability

C. Considering risk factors that can be quantified
D. Managing the risk by using controls

Answer: A

NEW QUESTION 823
- (Exam Topic 2)
Which of the following is MOST influential when management makes risk response decisions?

A. Risk appetite
B. Audit risk
C. Residual risk
D. Detection risk

Answer: A

NEW QUESTION 825
- (Exam Topic 2)
Which of the following is the BEST way to ensure ongoing control effectiveness?

A. Establishing policies and procedures
B. Periodically reviewing control design
C. Measuring trends in control performance
D. Obtaining management control attestations

Answer: C

NEW QUESTION 829
- (Exam Topic 2)
The GREATEST concern when maintaining a risk register is that:

A. impacts are recorded in qualitative terms.
B. executive management does not perform periodic reviews.
C. IT risk is not linked with IT assets.
D. significant changes in risk factors are excluded.

Answer: D

NEW QUESTION 832
- (Exam Topic 2)
The PRIMARY purpose of using control metrics is to evaluate the:

A. amount of risk reduced by compensating controls.
B. amount of risk present in the organization.
C. variance against objectives.
D. number of incidents.

Answer: C

NEW QUESTION 834
- (Exam Topic 2)
The BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability remediation program is the number of:

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

Answer: C

NEW QUESTION 835
- (Exam Topic 2)
Which of the following would MOST likely cause a risk practitioner to reassess risk scenarios?

A. A change in the risk management policy
B. A major security incident
C. A change in the regulatory environment
D. An increase in intrusion attempts

Answer: C

NEW QUESTION 837
- (Exam Topic 2)
What can be determined from the risk scenario chart?

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

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

Answer: A

NEW QUESTION 841
- (Exam Topic 2)
A department has been granted an exception to bypass the existing approval process for purchase orders. The risk practitioner should verify the exception has been approved by which of the following?

A. Internal audit
B. Control owner
C. Senior management
D. Risk manager

Answer: B

NEW QUESTION 844
- (Exam Topic 2)
Which of the following is MOST likely to be impacted as a result of a new policy which allows staff members to remotely connect to the organization's IT systems via personal or public computers?

A. Risk appetite
B. Inherent risk
C. Key risk indicator (KRI)
D. Risk tolerance

Answer: B

NEW QUESTION 848
- (Exam Topic 2)
Which of the following will BEST help to ensure that information system controls are effective?

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

Answer: C

NEW QUESTION 852
- (Exam Topic 2)
The annualized loss expectancy (ALE) method of risk analysis:

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

Answer: C

NEW QUESTION 854
- (Exam Topic 2)
An IT operations team implements disaster recovery controls based on decisions from application owners regarding the level of resiliency needed. Who is the risk owner in this scenario?

A. Business resilience manager
B. Disaster recovery team lead
C. Application owner
D. IT operations manager

Answer: C

NEW QUESTION 858
- (Exam Topic 2)
Implementing which of the following will BEST help ensure that systems comply with an established baseline before deployment?

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

Answer: C

NEW QUESTION 863
- (Exam Topic 2)
Which of the following should be the PRIMARY objective of a risk awareness training program?

A. To enable risk-based decision making
B. To promote awareness of the risk governance function
C. To clarify fundamental risk management principles
D. To ensure sufficient resources are available

Answer: A

NEW QUESTION 864
- (Exam Topic 2)
Which of the following criteria is MOST important when developing a response to an attack that would compromise data?

A. The recovery time objective (RTO)
B. The likelihood of a recurring attack
C. The organization's risk tolerance
D. The business significance of the information

Answer: D

NEW QUESTION 869
- (Exam Topic 2)
A risk practitioner recently discovered that sensitive data from the production environment is required for testing purposes in non-production environments. Which of the following i the BEST recommendation to address this situation?

A. Enable data encryption in the test environment
B. Implement equivalent security in the test environment.
C. Prevent the use of production data for test purposes
D. Mask data before being transferred to the test environment.

Answer: B

NEW QUESTION 874
- (Exam Topic 2)
A maturity model will BEST indicate:

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

Answer: B

NEW QUESTION 879
- (Exam Topic 2)
Which of the following is the MOST effective way to mitigate identified risk scenarios?

A. Assign ownership of the risk response plan
B. Provide awareness in early detection of risk.
C. Perform periodic audits on identified risk.
D. areas Document the risk tolerance of the organization.

Answer: A

NEW QUESTION 880
- (Exam Topic 2)
Which of the following would qualify as a key performance indicator (KPI)?

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

Answer:

B

NEW QUESTION 882
- (Exam Topic 2)
An organization has outsourced a critical process involving highly regulated data to a third party with servers located in a foreign country. Who is accountable for the confidentiality of this data?

A. Third-party data custodian
B. Data custodian
C. Regional office executive
D. Data owner

Answer: D

NEW QUESTION 886
- (Exam Topic 2)
An organization striving to be on the leading edge in regard to risk monitoring would MOST likely implement:

A. procedures to monitor the operation of controls.
B. a tool for monitoring critical activities and controls.
C. real-time monitoring of risk events and control exceptions.
D. monitoring activities for all critical assets.
E. Perform a controls assessment.

Answer: C

NEW QUESTION 887
- (Exam Topic 2)
Which of the following is the BEST way for a risk practitioner to verify that management has addressed control issues identified during a previous external audit?

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

Answer: B

NEW QUESTION 892
- (Exam Topic 2)
Which of the following should management consider when selecting a risk mitigation option?

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

Answer: B

NEW QUESTION 896
- (Exam Topic 2)
The risk associated with a high-risk vulnerability in an application is owned by the:

A. security department.
B. business unit
C. vendor.
D. IT department.

Answer: B

NEW QUESTION 901
- (Exam Topic 2)
Which of the following is the MOST important consideration when determining whether to accept residual risk after security controls have been implemented on a critical system?

A. Cost versus benefit of additional mitigating controls
B. Annualized loss expectancy (ALE) for the system
C. Frequency of business impact
D. Cost of the Information control system

Answer: A

NEW QUESTION 903
- (Exam Topic 2)
Which of the following should be the MAIN consideration when validating an organization's risk appetite?

A. Comparison against regulations

B. Maturity of the risk culture
C. Capacity to withstand loss
D. Cost of risk mitigation options

Answer: B

NEW QUESTION 906
- (Exam Topic 2)
Which of the following is the GREATEST risk associated with the transition of a sensitive data backup solution from on-premise to a cloud service provider?

A. More complex test restores
B. Inadequate service level agreement (SLA) with the provider
C. More complex incident response procedures
D. Inadequate data encryption

Answer: D

NEW QUESTION 909
- (Exam Topic 2)
Which of the following should a risk practitioner do FIRST when an organization decides to use a cloud service?

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

Answer: D

NEW QUESTION 914
- (Exam Topic 2)
The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:

A. rectify errors in results of KRIs.
B. detect changes in the risk profile.
C. reduce costs of risk mitigation controls.
D. continually improve risk assessments.

Answer: B

NEW QUESTION 919
- (Exam Topic 2)
Which of The following will BEST communicate the importance of risk mitigation initiatives to senior management?

A. Business case
B. Balanced scorecard
C. Industry standards
D. Heat map

Answer: A

NEW QUESTION 924
- (Exam Topic 2)
Which of the following is the PRIMARY reason for an organization to ensure the risk register is updated regularly?

A. Risk assessment results are accessible to senior management and stakeholders.
B. Risk mitigation activities are managed and coordinated.
C. Key risk indicators (KRIs) are evaluated to validate they are still within the risk threshold.
D. Risk information is available to enable risk-based decisions.

Answer: D

NEW QUESTION 927
- (Exam Topic 2)
The BEST criteria when selecting a risk response is the:

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

Answer: C

NEW QUESTION 932
- (Exam Topic 2)
Which of the following would BEST enable mitigation of newly identified risk factors related to internet of Things (IoT)?

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

Answer: A

NEW QUESTION 936
- (Exam Topic 2)
When establishing leading indicators for the information security incident response process it is MOST important to consider the percentage of reported incidents:

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

Answer: C

NEW QUESTION 939
- (Exam Topic 2)
Which of the following is the BEST course of action when risk is found to be above the acceptable risk appetite?

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

Answer: D

NEW QUESTION 942
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

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 FirstTry

* CRISC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CRISC Practice Test Here