Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (Exam Topic 4)
A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?

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

Answer: C

NEW QUESTION 2
- (Exam Topic 4)
What is the MAIN benefit of using a top-down approach to develop risk scenarios?

A. It describes risk events specific to technology used by the enterprise.
B. It establishes the relationship between risk events and organizational objectives.
C. It uses hypothetical and generic risk events specific to the enterprise.
D. It helps management and the risk practitioner to refine risk scenarios.

Answer: C

NEW QUESTION 3
- (Exam Topic 4)
An organization's business gap analysis reveals the need for a robust IT risk strategy. Which of the following should be the risk practitioner's PRIMARY consideration when participating in development of the new strategy?

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

Answer: C

NEW QUESTION 4
- (Exam Topic 4)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 5
- (Exam Topic 4)
WhichT5f the following is the MOST effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage?

A. Enforce sanctions for noncompliance with security procedures.
B. Conduct organization-w>de phishing simulations.
C. Require training on the data handling policy.
D. Require regular testing of the data breach response plan.

Answer: B

NEW QUESTION 6
- (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 7
- (Exam Topic 4)
Which of the following key performance indicators (KPis) would BEST measure me risk of a service outage when using a Software as a Service (SaaS) vendors

A. Frequency of business continuity plan (BCP) lasting
B. Frequency and number of new software releases

C. Frequency and duration of unplanned downtime
D. Number of IT support staff available after business hours

Answer: C

NEW QUESTION 8
- (Exam Topic 4)
Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

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

Answer: D

NEW QUESTION 9
- (Exam Topic 4)
A risk practitioner notices a risk scenario associated with data loss at the organization's cloud provider is assigned to the provider Who should the risk scenario be reassigned to?

A. Senior management
B. Chief risk officer (CRO)
C. Vendor manager
D. Data owner

Answer: D

NEW QUESTION 10
- (Exam Topic 4)
Which of the following is the GREATEST benefit of using IT risk scenarios?

A. They support compliance with regulations.
B. They provide evidence of risk assessment.
C. They facilitate communication of risk.
D. They enable the use of key risk indicators (KRIs)

Answer: C

NEW QUESTION 10
- (Exam Topic 4)
A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

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

Answer: B

NEW QUESTION 12
- (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 16
- (Exam Topic 4)
A root because analysis indicates a major service disruption due to a lack of competency of newly hired IT system administrators Who should be accountable for resolving the situation?

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

Answer: C

NEW QUESTION 21
- (Exam Topic 4)

If preventive controls cannot be Implemented due to technology limitations, which of the following should be done FIRST to reduce risk7

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

Answer: A

NEW QUESTION 24
- (Exam Topic 4)
An organization uses one centralized single sign-on (SSO) control to cover many applications. Which of the following is the BEST course of action when a new application is added to the environment after testing of the SSO control has been completed?

A. Initiate a retest of the full control
B. Retest the control using the new application as the only sample.
C. Review the corresponding change control documentation
D. Re-evaluate the control during (he next assessment

Answer: A

NEW QUESTION 25
- (Exam Topic 4)
Which of the following would be a risk practitioner's GREATEST concern with the use of a vulnerability scanning tool?

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

Answer: B

NEW QUESTION 26
- (Exam Topic 4)
Which of the following is the MOST effective way to help ensure accountability for managing risk?

A. Assign process owners to key risk areas.
B. Obtain independent risk assessments.
C. Assign incident response action plan responsibilities.
D. Create accurate process narratives.

Answer: A

NEW QUESTION 31
- (Exam Topic 4)
Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

A. Gap analysis
B. Threat assessment
C. Resource skills matrix
D. Data quality assurance plan

Answer: A

NEW QUESTION 35
- (Exam Topic 4)
Which of the following is the BEST approach for an organization in a heavily regulated industry to comprehensively test application functionality?

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

Answer: D

NEW QUESTION 40
- (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 45
- (Exam Topic 4)
A recent regulatory requirement has the potential to affect an organization's use of a third party to supply outsourced business services. Which of the following is the BEST course of action?

A. Conduct a gap analysis.
B. Terminate the outsourcing agreement.
C. Identify compensating controls.
D. Transfer risk to the third party.

Answer: A

NEW QUESTION 48
- (Exam Topic 4)
Which of The following BEST represents the desired risk posture for an organization?

A. Inherent risk is lower than risk tolerance.
B. Operational risk is higher than risk tolerance.
C. Accepted risk is higher than risk tolerance.
D. Residual risk is lower than risk tolerance.

Answer: D

NEW QUESTION 51
- (Exam Topic 3)
Which of the following BEST measures the impact of business interruptions caused by an IT service outage?

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

Answer: A

NEW QUESTION 56
- (Exam Topic 3)
Which of The following should be of GREATEST concern for an organization considering the adoption of a bring your own device (BYOD) initiative?

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

Answer: B

NEW QUESTION 59
- (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 64
- (Exam Topic 4)
Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?

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

Answer: A

NEW QUESTION 66
- (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 69
- (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 72
- (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 75
- (Exam Topic 4)
Which of the following is MOST important to consider before determining a response to a vulnerability?

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

Answer: C

NEW QUESTION 79
- (Exam Topic 4)
A legacy application used for a critical business function relies on software that has reached the end of extended support Which of the following is the MOST effective control to manage this application?

A. Subscribe to threat intelligence to monitor external attacks.
B. Apply patches for a newer version of the application.
C. Segment the application within the existing network.
D. Increase the frequency of regular system and data backups.

Answer: D

NEW QUESTION 80
- (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 84
- (Exam Topic 3)
The BEST way to improve a risk register is to ensure the register:

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

Answer: A

NEW QUESTION 89
- (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 90
- (Exam Topic 3)
An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course of action?

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

Answer: B

NEW QUESTION 91
- (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)
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 97
- (Exam Topic 3)
Which of the following is MOST important to include in a risk assessment of an emerging technology?

A. Risk response plans
B. Risk and control ownership
C. Key controls
D. Impact and likelihood ratings

Answer: D

NEW QUESTION 99
- (Exam Topic 3)
Which of the following controls are BEST strengthened by a clear organizational code of ethics?

A. Detective controls
B. Administrative controls
C. Technical controls
D. Preventive controls

Answer: B

NEW QUESTION 101
- (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 105

- (Exam Topic 3)
Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

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

Answer: B

NEW QUESTION 109
- (Exam Topic 3)
A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

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

Answer: A

NEW QUESTION 111
- (Exam Topic 3)
Which of the following will help ensure the elective decision-making of an IT risk management committee?

A. Key stakeholders are enrolled as members
B. Approved minutes ate forwarded to senior management
C. Committee meets at least quarterly
D. Functional overlap across the business is minimized

Answer: D

NEW QUESTION 116
- (Exam Topic 3)
The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:

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

Answer: A

NEW QUESTION 118
- (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 121
- (Exam Topic 3)
Which of the following would require updates to an organization's IT risk register?

A. Discovery of an ineffectively designed key IT control
B. Management review of key risk indicators (KRIs)
C. Changes to the team responsible for maintaining the register
D. Completion of the latest internal audit

Answer: A

NEW QUESTION 123
- (Exam Topic 3)
Which of tie following is We MOST important consideration when implementing ethical remote work monitoring?

A. Monitoring is only conducted between official hours of business
B. Employees are informed of how they are bong monitored
C. Reporting on nonproductive employees is sent to management on a scheduled basis
D. Multiple data monitoring sources are integrated into security incident response procedures

Answer: B

NEW QUESTION 128
- (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 129
- (Exam Topic 3)
Which of the following should be an element of the risk appetite of an organization?

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

Answer: B

NEW QUESTION 130
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?

A. Percentage of high-risk vulnerabilities missed
B. Number of high-risk vulnerabilities outstanding
C. Defined thresholds for high-risk vulnerabilities
D. Percentage of high-risk vulnerabilities addressed

Answer: D

NEW QUESTION 131
- (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 135
- (Exam Topic 3)
Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

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

Answer: B

NEW QUESTION 139
- (Exam Topic 3)
A service provider is managing a client’s servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider’s MOST appropriate action would be to:

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

Answer: D

NEW QUESTION 143
- (Exam Topic 3)
Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

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

Answer: C

NEW QUESTION 146
- (Exam Topic 3)
An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

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

Answer: A

NEW QUESTION 147
- (Exam Topic 3)
Which of the following is the PRIMARY benefit of using an entry in the risk register to track the aggregate risk associated with server failure?

A. It provides a cost-benefit analysis on control options available for implementation.
B. It provides a view on where controls should be applied to maximize the uptime of servers.
C. It provides historical information about the impact of individual servers malfunctioning.
D. It provides a comprehensive view of the impact should the servers simultaneously fail.

Answer: D

NEW QUESTION 148
- (Exam Topic 3)
Which of the following is the BEST indication of a mature organizational risk culture?

A. Corporate risk appetite is communicated to staff members.
B. Risk owners understand and accept accountability for risk.
C. Risk policy has been published and acknowledged by employees.
D. Management encourages the reporting of policy breaches.

Answer: B

NEW QUESTION 150
- (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 154
- (Exam Topic 3)
Determining if organizational risk is tolerable requires:

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

Answer: D

NEW QUESTION 156
- (Exam Topic 3)
Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?

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

Answer: B

NEW QUESTION 161
- (Exam Topic 3)
Which of the following should be determined FIRST when a new security vulnerability is made public?

A. Whether the affected technology is used within the organization
B. Whether the affected technology is Internet-facing

C. What mitigating controls are currently in place
D. How pervasive the vulnerability is within the organization

Answer: A

NEW QUESTION 165
- (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 170
- (Exam Topic 3)
Which of the following is the MOST effective way to incorporate stakeholder concerns when developing risk scenarios?

A. Evaluating risk impact
B. Establishing key performance indicators (KPIs)
C. Conducting internal audits
D. Creating quarterly risk reports

Answer: A

NEW QUESTION 175
- (Exam Topic 3)
The MOST important objective of information security controls is to:

A. Identify threats and vulnerability
B. Ensure alignment with industry standards
C. Provide measurable risk reduction
D. Enforce strong security solutions

Answer: C

NEW QUESTION 176
- (Exam Topic 3)
Which of the following should be of GREATEST concern lo a risk practitioner reviewing the implementation of an emerging technology?

A. Lack of alignment to best practices
B. Lack of risk assessment
C. Lack of risk and control procedures
D. Lack of management approval

Answer: B

NEW QUESTION 179
- (Exam Topic 3)
Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

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

Answer: D

NEW QUESTION 180
- (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 184
- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 187
- (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 190
- (Exam Topic 3)
Which of the following BEST indicates whether security awareness training is effective?

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

Answer: B

NEW QUESTION 195
- (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 199
- (Exam Topic 3)
Which of the following scenarios represents a threat?

A. Connecting a laptop to a free, open, wireless access point (hotspot)
B. Visitors not signing in as per policy
C. Storing corporate data in unencrypted form on a laptop
D. A virus transmitted on a USB thumb drive

Answer: D

NEW QUESTION 200
- (Exam Topic 3)
Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information lo a supplier?

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

Answer: B

NEW QUESTION 201
- (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 202
- (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 204
- (Exam Topic 3)
Which of the following provides the MOST useful information when determining if a specific control should be implemented?

A. Business impact analysis (BIA)
B. Cost-benefit analysis
C. Attribute analysis
D. Root cause analysis

Answer: B

NEW QUESTION 209
- (Exam Topic 3)
Which of the following is the PRIMARY reason to use key control indicators (KCIs) to evaluate control operating effectiveness?

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

Answer: C

NEW QUESTION 211
- (Exam Topic 3)
Which of the following roles is BEST suited to help a risk practitioner understand the impact of IT-related events on business objectives?

A. IT management
B. Internal audit
C. Process owners
D. Senior management

Answer: C

NEW QUESTION 214
- (Exam Topic 3)
Vulnerabilities have been detected on an organization's systems. Applications installed on these systems will not operate if the underlying servers are updated. Which of the following is the risk practitioner's BEST course of action?

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

Answer: D

NEW QUESTION 216
- (Exam Topic 3)
Which of The following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?

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

Answer: C

NEW QUESTION 217
- (Exam Topic 3)
Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

A. Obtain objective assessment of the control environment.
B. Ensure the risk profile is defined and communicated.
C. Validate the threat management process.
D. Obtain an objective view of process gaps and systemic errors.

Answer: A

NEW QUESTION 221
- (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 223
- (Exam Topic 3)
Which of the following is the BEST Key control indicator KCO to monitor the effectiveness of patch management?

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

Answer: D

NEW QUESTION 224
- (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 226
- (Exam Topic 3)
While reviewing the risk register, a risk practitioner notices that different business units have significant variances in inherent risk for the same risk scenario. Which of the following is the BEST course of action?

A. Update the risk register with the average of residual risk for both business units.
B. Review the assumptions of both risk scenarios to determine whether the variance is reasonable.
C. Update the risk register to ensure both risk scenarios have the highest residual risk.
D. Request that both business units conduct another review of the risk.

Answer: B

NEW QUESTION 231
- (Exam Topic 3)
The risk associated with an asset after controls are applied can be expressed as:

A. a function of the cost and effectiveness of controls.
B. the likelihood of a given threat.
C. a function of the likelihood and impact.
D. the magnitude of an impact.

Answer: C

NEW QUESTION 234
- (Exam Topic 3)
Winch of the following key control indicators (KCIs) BEST indicates whether security requirements are identified and managed throughout a project He cycle?

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

Answer: A

NEW QUESTION 235
- (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 237
- (Exam Topic 3)
Which of the following is the BEST way to mitigate the risk to IT infrastructure availability?

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

Answer: D

NEW QUESTION 241
- (Exam Topic 3)
Which of the following practices MOST effectively safeguards the processing of personal data?

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

Answer: B

NEW QUESTION 243
- (Exam Topic 3)
Key risk indicators (KRIs) are MOST useful during which of the following risk management phases?

A. Monitoring
B. Analysis
C. Identification
D. Response selection

Answer: A

NEW QUESTION 248
- (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 251
- (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 256
- (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 259
- (Exam Topic 3)
When reviewing a business continuity plan (BCP). which of the following would be the MOST significant deficiency?

A. BCP testing is net in conjunction with the disaster recovery plan (DRP)
B. Recovery time objectives (RTOs) do not meet business requirements.
C. BCP is often tested using the walk-through method.
D. Each business location has separate, inconsistent BCPs.

Answer: B

NEW QUESTION 264
- (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 269
- (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 272
- (Exam Topic 3)
Winch of the following is the BEST evidence of an effective risk treatment plan?

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

Answer: B

NEW QUESTION 273
- (Exam Topic 3)
An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?

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

Answer: B

NEW QUESTION 278
- (Exam Topic 3)
Which of the following is MOST important to the integrity of a security log?

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

Answer: B

NEW QUESTION 280
- (Exam Topic 3)
Which of the following is the GREATEST risk associated with the misclassification of data?

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

Answer: A

NEW QUESTION 284

- (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 285
- (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 286
- (Exam Topic 3)
Which of the following is the MOST important component in a risk treatment plan?

A. Technical details
B. Target completion date
C. Treatment plan ownership
D. Treatment plan justification

Answer: D

NEW QUESTION 290
- (Exam Topic 3)
The PRIMARY objective of a risk identification process is to:

A. evaluate how risk conditions are managed.
B. determine threats and vulnerabilities.
C. estimate anticipated financial impact of risk conditions.
D. establish risk response options.

Answer: B

NEW QUESTION 295
- (Exam Topic 3)
Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

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

Answer: C

NEW QUESTION 297
- (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 299
- (Exam Topic 3)
Which of the following is MOST important to the successful development of IT risk scenarios?

A. Cost-benefit analysis
B. Internal and external audit reports
C. Threat and vulnerability analysis
D. Control effectiveness assessment

Answer: C

NEW QUESTION 304
- (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 307
- (Exam Topic 3)
What should be the PRIMARY driver for periodically reviewing and adjusting key risk indicators (KRIs)?

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

Answer: B

NEW QUESTION 312
- (Exam Topic 3)
Who should be accountable for monitoring the control environment to ensure controls are effective?

A. Risk owner
B. Security monitoring operations
C. Impacted data owner
D. System owner

Answer: A

NEW QUESTION 317
- (Exam Topic 3)
Which of the following BEST facilities the alignment of IT risk management with enterprise risk management (ERM)?

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

Answer: C

NEW QUESTION 320
- (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 323
- (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 324
- (Exam Topic 3)
Which of the following risk management practices BEST facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register?

A. Key risk indicators (KRIs) are developed for key IT risk scenarios
B. IT risk scenarios are assessed by the enterprise risk management team
C. Risk appetites for IT risk scenarios are approved by key business stakeholders.
D. IT risk scenarios are developed in the context of organizational objectives.

Answer: D

NEW QUESTION 329
- (Exam Topic 3)
To communicate the risk associated with IT in business terms, which of the following MUST be defined?

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

Answer: C

NEW QUESTION 331
- (Exam Topic 3)
The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

A. stakeholder risk tolerance.
B. benchmarking criteria.
C. suppliers used by the organization.
D. the control environment.

Answer: D

NEW QUESTION 334
- (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 336
- (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 337
- (Exam Topic 3)
Which of the following is the GREATEST advantage of implementing a risk management program?

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

Answer: A

NEW QUESTION 340
- (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 341
- (Exam Topic 3)
A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

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

Answer: B

NEW QUESTION 342
- (Exam Topic 3)
An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:

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

Answer: D

NEW QUESTION 343
- (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 346
- (Exam Topic 3)
Which of the following BEST enforces access control for an organization that uses multiple cloud technologies?

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

Answer: C

NEW QUESTION 349
- (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 353
- (Exam Topic 3)
Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

A. Compliance breaches are addressed in a timely manner.
B. Risk ownership is identified and assigned.
C. Risk treatment options receive adequate funding.
D. Residual risk is within risk tolerance.

Answer: B

NEW QUESTION 356
- (Exam Topic 3)
Which of The following should be the FIRST step when a company is made aware of new regulatory requirements impacting IT?

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

Answer: C

NEW QUESTION 361
- (Exam Topic 3)
Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

A. Percentage of unpatched IT assets

B. Percentage of IT assets without ownership
C. The number of IT assets securely disposed during the past year
D. The number of IT assets procured during the previous month

Answer: B

NEW QUESTION 366
- (Exam Topic 4)
The objective of aligning mitigating controls to risk appetite is to ensure that:

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

Answer: D

NEW QUESTION 368
- (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 373
- (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 375
- (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 377
- (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 380
- (Exam Topic 4)
A company has recently acquired a customer relationship management (CRM) application from a certified software vendor. Which of the following will BE ST help lo prevent technical vulnerabilities from being exploded?

A. implement code reviews and Quality assurance on a regular basis
B. Verity me software agreement indemnifies the company from losses
C. Review the source coda and error reporting of the application
D. Update the software with the latest patches and updates

Answer: D

NEW QUESTION 382

- (Exam Topic 4)
Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?

A. Data classification policy
B. Emerging technology trends
C. The IT strategic plan
D. The risk register

Answer: C

NEW QUESTION 385
- (Exam Topic 4)
A risk practitioner recently discovered that personal information from the production environment is required for testing purposes in non-production environments. Which of the following is the BEST recommendation to address this situation?

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

Answer: C

NEW QUESTION 387
- (Exam Topic 4)
Reviewing which of the following BEST helps an organization gam insight into its overall risk profile"

A. Risk register
B. Risk appetite
C. Threat landscape
D. Risk metrics

Answer: B

NEW QUESTION 392
- (Exam Topic 4)
Which of the following is the BEST way to ensure adequate resources will be allocated to manage identified risk?

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

Answer: D

NEW QUESTION 395
- (Exam Topic 4)
Which of the following BEST enables a risk practitioner to understand management's approach to organizational risk?

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

Answer: B

NEW QUESTION 398
- (Exam Topic 4)
Which of the following will BEST help to ensure the continued effectiveness of the IT risk management function within an organization experiencing high employee turnover?

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

Answer: B

NEW QUESTION 400
- (Exam Topic 4)
An organization has agreed to a 99% availability for its online services and will not accept availability that falls below 98.5%. This is an example of:

A. risk mitigation.
B. risk evaluation.
C. risk appetite.
D. risk tolerance.

Answer: C

NEW QUESTION 405
- (Exam Topic 4)
Which of the following BEST enables senior management lo compare the ratings of risk scenarios?

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

Answer: D

NEW QUESTION 409
- (Exam Topic 4)
Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board"

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

Answer: C

NEW QUESTION 411
- (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 414
- (Exam Topic 4)
Which of the following will BEST help to ensure new IT policies address the enterprise's requirements?

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

Answer: B

NEW QUESTION 418
- (Exam Topic 4)
Which of the following would BEST facilitate the implementation of data classification requirements?

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

Answer: A

NEW QUESTION 422
- (Exam Topic 4)
Which of the following activities BEST facilitates effective risk management throughout the organization?

A. Reviewing risk-related process documentation
B. Conducting periodic risk assessments
C. Performing a business impact analysis (BIA)
D. Performing frequent audits

Answer: B

NEW QUESTION 425
- (Exam Topic 4)
Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

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

Answer:

B

NEW QUESTION 426
- (Exam Topic 4)
When of the following standard operating procedure (SOP) statements BEST illustrates appropriate risk register maintenance?

A. Remove risk that has been mitigated by third-party transfer
B. Remove risk that management has decided to accept
C. Remove risk only following a significant change in the risk environment
D. Remove risk when mitigation results in residual risk within tolerance levels

Answer: C

NEW QUESTION 427
- (Exam Topic 4)
Which of the following would be a risk practitioner's BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

A. Perform a gap analysis
B. Conduct system testing
C. Implement compensating controls
D. Update security policies

Answer: A

NEW QUESTION 429
- (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 433
- (Exam Topic 4)
What is the PRIMARY reason an organization should include background checks on roles with elevated access to production as part of its hiring process?

A. Reduce internal threats
B. Reduce exposure to vulnerabilities
C. Eliminate risk associated with personnel
D. Ensure new hires have the required skills

Answer: C

NEW QUESTION 435
- (Exam Topic 4)
Which of the following potential scenarios associated with the implementation of a new database technology presents the GREATEST risk to an organization?

A. The organization may not have a sufficient number of skilled resources.
B. Application and data migration cost for backups may exceed budget.
C. Data may not be recoverable due to system failures.
D. The database system may not be scalable in the future.

Answer: B

NEW QUESTION 438
- (Exam Topic 4)
Which of the following is the PRIMARY reason for sharing risk assessment reports with senior stakeholders?

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

Answer: A

NEW QUESTION 439
- (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 444
- (Exam Topic 4)
During an acquisition, which of the following would provide the MOST useful input to the parent company's risk practitioner when developing risk scenarios for the post-acquisition phase?

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

Answer: C

NEW QUESTION 447
- (Exam Topic 4)
An incentive program is MOST likely implemented to manage the risk associated with loss of which organizational asset?

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

Answer: A

NEW QUESTION 451
- (Exam Topic 4)
Which of the following BEST enables effective IT control implementation?

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

Answer: B

NEW QUESTION 456
- (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 461
- (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 462
- (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 464

- (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 467
- (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 469
- (Exam Topic 4)
One of an organization's key IT systems cannot be patched because the patches interfere with critical business application functionalities. Which of the following would be the risk practitioner's BEST recommendation?

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

Answer: A

NEW QUESTION 470
- (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 475
- (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 480
- (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 483
- (Exam Topic 4)
When confirming whether implemented controls are operating effectively, which of the following is MOST important to review?

A. Results of benchmarking studies
B. Results of risk assessments
C. Number of emergency change requests
D. Maturity model

Answer: B

NEW QUESTION 488
- (Exam Topic 4)
Which of the following would BEST mitigate an identified risk scenario?

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

Answer: C

NEW QUESTION 493
- (Exam Topic 4)
A global organization has implemented an application that does not address all privacy requirements across multiple jurisdictions. Which of the following risk responses has the organization adopted with regard to privacy requirements?

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

Answer: A

NEW QUESTION 494
- (Exam Topic 4)
To define the risk management strategy which of the following MUST be set by the board of directors?

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

Answer: B

NEW QUESTION 495
- (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 500
- (Exam Topic 4)
Which of the blowing is MOST important when implementing an organization s security policy?

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

Answer: A

NEW QUESTION 501
- (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 504
- (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 505
- (Exam Topic 4)
When documenting a risk response, which of the following provides the STRONGEST evidence to support the decision?

A. Verbal majority acceptance of risk by committee
B. List of compensating controls
C. IT audit follow-up responses
D. A memo indicating risk acceptance

Answer: C

NEW QUESTION 506
- (Exam Topic 4)
An organization control environment is MOST effective when:

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

Answer: B

NEW QUESTION 509
- (Exam Topic 4)
Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

A. Increase in mitigating control costs
B. Increase in risk event impact
C. Increase in risk event likelihood
D. Increase in cybersecurity premium

Answer: C

NEW QUESTION 512
- (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 513
- (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 515
- (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 517
- (Exam Topic 4)
Who is MOST appropriate to be assigned ownership of a control

A. The individual responsible for control operation
B. The individual informed of the control effectiveness
C. The individual responsible for resting the control

D. The individual accountable for monitoring control effectiveness

Answer: D

NEW QUESTION 522
- (Exam Topic 4)
When defining thresholds for control key performance indicators (KPIs). it is MOST helpful to align:

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

Answer: B

NEW QUESTION 526
- (Exam Topic 4)
A risk practitioner observed Vial a high number of pokey exceptions were approved by senior management. Which of the following is the risk practitioner's BEST course of action to determine root cause?

A. Review the risk profile
B. Review pokey change history
C. interview the control owner
D. Perform control testing

Answer: C

NEW QUESTION 527
- (Exam Topic 4)
Which of the following should be considered FIRST when creating a comprehensive IT risk register?

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

Answer: C

NEW QUESTION 532
- (Exam Topic 4)
When reviewing the business continuity plan (BCP) of an online sales order system, a risk practitioner notices that the recovery time objective (RTO) has a shorter lime than what is defined in the disaster recovery plan (DRP). Which of the following is the BEST way for the risk practitioner to address this concern?

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

Answer: D

NEW QUESTION 537
- (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 540
- (Exam Topic 4)
Which of the following is the BEST way to help ensure risk will be managed properly after a business process has been re-engineered?

A. Reassessing control effectiveness of the process
B. Conducting a post-implementation review to determine lessons learned
C. Reporting key performance indicators (KPIs) for core processes
D. Establishing escalation procedures for anomaly events

Answer: A

NEW QUESTION 541
- (Exam Topic 4)
An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely

lead to architecture and design trade-offs?

A. Acquisition
B. Implementation
C. Initiation
D. Operation and maintenance

Answer: C

NEW QUESTION 543
- (Exam Topic 4)
Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

A. The report was provided directly from the vendor.
B. The risk associated with multiple control gaps was accepted.
C. The control owners disagreed with the auditor's recommendations.
D. The controls had recurring noncompliance.

Answer: A

NEW QUESTION 546
- (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 548
- (Exam Topic 4)
Which of the following is MOST important to promoting a risk-aware culture?

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

Answer: D

NEW QUESTION 553
- (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 556
- (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 561
- (Exam Topic 4)
Which of the following is the PRIMARY objective of maintaining an information asset inventory?

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

Answer: B

NEW QUESTION 563
- (Exam Topic 4)
Which of the following is MOST helpful in providing an overview of an organization's risk management program?

A. Risk management treatment plan
B. Risk assessment results
C. Risk management framework
D. Risk register

Answer: C

NEW QUESTION 565
- (Exam Topic 4)
Which of the following is the BEST approach for selecting controls to minimize risk?

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

Answer: C

NEW QUESTION 569
- (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 571
- (Exam Topic 4)
Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

A. Ability to determine business impact
B. Up-to-date knowledge on risk responses
C. Decision-making authority for risk treatment
D. Awareness of emerging business threats

Answer: A

NEW QUESTION 572
- (Exam Topic 4)
Which of the following is the PRIMARY objective of establishing an organization's risk tolerance and appetite?

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

Answer: B

NEW QUESTION 576
- (Exam Topic 4)
Which of the following would be the BEST way for a risk practitioner to validate the effectiveness of a patching program?

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

Answer: C

NEW QUESTION 581
- (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 583
- (Exam Topic 4)
Effective risk communication BEST benefits an organization by:

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

Answer: A

NEW QUESTION 587
- (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 590
- (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 591
- (Exam Topic 4)
A risk practitioner has established that a particular control is working as desired, but the annual cost of maintenance has increased and now exceeds the expected annual loss exposure. The result is that the control is:

A. mature
B. ineffective.
C. optimized.
D. inefficient.

Answer: B

NEW QUESTION 592
- (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 595
- (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 597
- (Exam Topic 4)
Who is the BEST person to the employee personal data?

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

Answer: A

NEW QUESTION 600
- (Exam Topic 4)
Which of the following should be accountable for ensuring that media containing financial information are adequately destroyed per an organization's data disposal policy?

A. Compliance manager
B. Data architect
C. Data owner
D. Chief information officer (CIO)

Answer: C

NEW QUESTION 601
- (Exam Topic 4)
Which of the following is the MOST useful information for a risk practitioner when planning response activities after risk identification?

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

Answer: B

NEW QUESTION 606
- (Exam Topic 4)
Which of the following would present the GREATEST challenge for a risk practitioner during a merger of two organizations?

A. Variances between organizational risk appetites
B. Different taxonomies to categorize risk scenarios
C. Disparate platforms for governance, risk, and compliance (GRC) systems
D. Dissimilar organizational risk acceptance protocols

Answer: A

NEW QUESTION 611
- (Exam Topic 4)
It is MOST important that security controls for a new system be documented in:

A. testing requirements
B. the implementation plan.
C. System requirements
D. The security policy

Answer: C

NEW QUESTION 613
- (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 617
- (Exam Topic 4)
Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

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

Answer: A

NEW QUESTION 619
- (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 623
- (Exam Topic 4)
Which of the following is the GREATEST concern when establishing key risk indicators (KRIs)?

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

Answer: B

NEW QUESTION 626
- (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 629
- (Exam Topic 4)
The MAIN purpose of selecting a risk response is to.

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

Answer: C

NEW QUESTION 634
- (Exam Topic 4)
Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?

A. Analyzing cyber intelligence reports
B. Engaging independent cybersecurity consultants
C. Increasing the frequency of updates to the risk register
D. Reviewing the outcome of the latest security risk assessment

Answer: D

NEW QUESTION 636
- (Exam Topic 4)
A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

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

Answer: B

NEW QUESTION 637
- (Exam Topic 4)
An organization recently implemented a machine learning-based solution to monitor IT usage and analyze user behavior in an effort to detect internal fraud. Which of the following is MOST likely to be reassessed as a result of this initiative?

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

Answer: A

NEW QUESTION 642

- (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 647
- (Exam Topic 4)
A bank recently incorporated Blockchain technology with the potential to impact known risk within the organization. Which of the following is the risk practitioner's BEST course of action?

A. Determine whether risk responses are still adequate.
B. Analyze and update control assessments with the new processes.
C. Analyze the risk and update the risk register as needed.
D. Conduct testing of the control that mitigate the existing risk.

Answer: B

NEW QUESTION 650
- (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 654
- (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 655
- (Exam Topic 4)
An internal audit report reveals that a legacy system is no longer supported Which of the following is the risk practitioner's MOST important action before recommending a risk response'

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

Answer: B

NEW QUESTION 660
- (Exam Topic 4)
The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.

Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading Internet leading to data compromise	Risk Council	End-User Computing Manager AND Inventory	IT Operations Manager AND Security Operations Manager	Low Likelihood	Very Serious	0 120	Mitigate	Purchase and acquire data encryption software for mobile
R003	Fire Hazard	A fire accident may destroy data center equipment and servers leading to loss of availability and services	Information Security Department	Data Center Facilities Manager	Facilities Manager	Low Likelihood	Serious	0 060	Transfer	Buy fire hazard insurance policy

A disgruntled			
Significant	0 10	Low Likelihood	0 30
Serious	0 20	Likely	0 50
Very Serious	0 40	Highly Likely	0 70
Catastrophic	0 80	Near Certainty	0 90

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

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

Answer: B

NEW QUESTION 665
- (Exam Topic 3)
Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

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

Answer: C

NEW QUESTION 668
- (Exam Topic 3)
A risk practitioner has just learned about new malware that has severely impacted industry peers worldwide data loss?

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

Answer: B

NEW QUESTION 670
- (Exam Topic 3)
Upon learning that the number of failed back-up attempts continually exceeds the current risk threshold, the risk practitioner should:

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

Answer: D

NEW QUESTION 671
- (Exam Topic 3)
To minimize the risk of a potential acquisition being exposed externally, an organization has selected a few

key employees to be engaged in the due diligence process. A member of the due diligence team realizes a close acquaintance is a high-ranking IT professional at a subsidiary of the company about to be acquired. What is the BEST course of action for this team member?

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

Answer: B

NEW QUESTION 672
- (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 677
- (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 679
- (Exam Topic 3)
Which of the following would be MOST helpful to an information security management team when allocating resources to mitigate exposures?

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

Answer: C

NEW QUESTION 683
- (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 687
- (Exam Topic 3)
A chief information officer (CIO) has identified risk associated with shadow systems being maintained by business units to address specific functionality gaps in the organization's enterprise resource planning (ERP) system. What is the BEST way to reduce this risk going forward?

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

Answer: B

NEW QUESTION 689
- (Exam Topic 3)
Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

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

Answer: C

NEW QUESTION 694
- (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 698
- (Exam Topic 3)
Which of the following is the MOST effective control to ensure user access is maintained on a least-privilege basis?

A. User authorization
B. User recertification
C. Change log review
D. Access log monitoring

Answer: B

NEW QUESTION 701
- (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 705
- (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 710
- (Exam Topic 3)
Which of the following is the STRONGEST indication an organization has ethics management issues?

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

Answer: A

NEW QUESTION 712
- (Exam Topic 3)
Which of the following BEST assists in justifying an investment in automated controls?

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

Answer: A

NEW QUESTION 713
- (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 716
- (Exam Topic 3)
The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

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

Answer: D

NEW QUESTION 717
- (Exam Topic 3)
Which of the following provides the BEST measurement of an organization's risk management maturity level?

A. Level of residual risk
B. The results of a gap analysis
C. IT alignment to business objectives
D. Key risk indicators (KRIs)

Answer: C

NEW QUESTION 721
- (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 724
- (Exam Topic 3)
The BEST reason to classify IT assets during a risk assessment is to determine the:

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

Answer: D

NEW QUESTION 729
- (Exam Topic 3)
The acceptance of control costs that exceed risk exposure MOST likely demonstrates:

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

Answer: C

NEW QUESTION 731
- (Exam Topic 3)
The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

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

Answer: A

NEW QUESTION 736
- (Exam Topic 3)
Which of the following is the BEST way to assess the effectiveness of an access management process?

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

Answer:

B

NEW QUESTION 737
- (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 741
- (Exam Topic 3)
Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?

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

Answer: A

NEW QUESTION 743
- (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 747
- (Exam Topic 3)
Which of the following will BEST help in communicating strategic risk priorities?

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

Answer: A

NEW QUESTION 751
- (Exam Topic 3)
Which of the following is the PRIMARY reason to adopt key control indicators (KCIs) in the risk monitoring and reporting process?

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

Answer: D

NEW QUESTION 752
- (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 753
- (Exam Topic 3)
Which of the following is the MOST common concern associated with outsourcing to a service provider?

A. Lack of technical expertise
B. Combining incompatible duties
C. Unauthorized data usage
D. Denial of service attacks

Answer: C

NEW QUESTION 757
- (Exam Topic 3)
Which of me following is MOST helpful to mitigate the risk associated with an application under development not meeting business objectives?

A. Identifying tweets that may compromise enterprise architecture (EA)
B. Including diverse Business scenarios in user acceptance testing (UAT)
C. Performing risk assessments during the business case development stage
D. Including key stakeholders in review of user requirements

Answer: D

NEW QUESTION 762
- (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 763
- (Exam Topic 3)
During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?

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

Answer: A

NEW QUESTION 764
- (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 768
- (Exam Topic 3)
An organization is implementing encryption for data at rest to reduce the risk associated with unauthorized access. Which of the following MUST be considered to assess the residual risk?

A. Data retention requirements
B. Data destruction requirements
C. Cloud storage architecture
D. Key management

Answer: D

NEW QUESTION 769
- (Exam Topic 3)
When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction based on:

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

Answer: A

NEW QUESTION 772
- (Exam Topic 3)
Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

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

Answer: B

NEW QUESTION 774
- (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 775
- (Exam Topic 3)
Which of the following should be the MOST important consideration when performing a vendor risk assessment?

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

Answer: B

NEW QUESTION 778
- (Exam Topic 3)
Management has required information security awareness training to reduce the risk associated with credential compromise. What is the BEST way to assess the effectiveness of the training?

A. Conduct social engineering testing.
B. Audit security awareness training materials.
C. Administer an end-of-training quiz.
D. Perform a vulnerability assessment.

Answer: A

NEW QUESTION 783
- (Exam Topic 3)
Which of the following is the MOST effective way to integrate risk and compliance management?

A. Embedding risk management into compliance decision-making
B. Designing corrective actions to improve risk response capabilities
C. Embedding risk management into processes that are aligned with business drivers
D. Conducting regular self-assessments to verify compliance

Answer: A

NEW QUESTION 785
- (Exam Topic 3)
While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

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

Answer: D

NEW QUESTION 787
- (Exam Topic 3)
Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (AI) solutions into the organization?

A. AI requires entirely new risk management processes.
B. AI potentially introduces new types of risk.
C. AI will result in changes to business processes.
D. Third-party AI solutions increase regulatory obligations.

Answer: B

NEW QUESTION 788
- (Exam Topic 3)
Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?

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

Answer: D

NEW QUESTION 793
- (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 794
- (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 799
- (Exam Topic 2)
A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner's FIRST course of action?

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

Answer: D

NEW QUESTION 803
- (Exam Topic 2)
Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?

A. Defining expectations in the enterprise risk policy
B. Increasing organizational resources to mitigate risks
C. Communicating external audit results
D. Avoiding risks that could materialize into substantial losses

Answer: A

NEW QUESTION 807
- (Exam Topic 2)
The purpose of requiring source code escrow in a contractual agreement is to:

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

Answer: B

NEW QUESTION 810
- (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 812
- (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 817
- (Exam Topic 2)
Which of the following BEST measures the efficiency of an incident response process?

A. Number of incidents escalated to management
B. Average time between changes and updating of escalation matrix
C. Average gap between actual and agreed response times
D. Number of incidents lacking responses

Answer: C

NEW QUESTION 820
- (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 822
- (Exam Topic 2)
A risk practitioner notices that a particular key risk indicator (KRI) has remained below its established trigger point for an extended period of time. Which of the following should be done FIRST?

A. Recommend a re-evaluation of the current threshold of the KRI.
B. Notify management that KRIs are being effectively managed.
C. Update the risk rating associated with the KRI In the risk register.
D. Update the risk tolerance and risk appetite to better align to the KRI.

Answer: A

NEW QUESTION 827
- (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 831
- (Exam Topic 2)
An organization's risk practitioner learns a new third-party system on the corporate network has introduced vulnerabilities that could compromise corporate IT systems. What should the risk practitioner do
FIRST?

A. Confirm the vulnerabilities with the third party
B. Identify procedures to mitigate the vulnerabilities.
C. Notify information security management.
D. Request IT to remove the system from the network.

Answer: B

NEW QUESTION 835
- (Exam Topic 2)
Which of the following is a crucial component of a key risk indicator (KRI) to ensure appropriate action is taken to mitigate risk?

A. Management intervention
B. Risk appetite
C. Board commentary
D. Escalation triggers

Answer: D

NEW QUESTION 840
- (Exam Topic 2)
Which of the following MUST be assessed before considering risk treatment options for a scenario with significant impact?

A. Risk magnitude
B. Incident probability
C. Risk appetite
D. Cost-benefit analysis

Answer: D

NEW QUESTION 841
- (Exam Topic 2)
A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?

A. Review the design of the machine learning model against control objectives.
B. Adopt the machine learning model as a replacement for current manual access reviews.
C. Ensure the model assists in meeting regulatory requirements for access controls.
D. Discourage the use of emerging technologies in key processes.

Answer: A

NEW QUESTION 844
- (Exam Topic 2)
Which of The following is the MOST relevant information to include in a risk management strategy?

A. Quantified risk triggers
B. Cost of controls
C. Regulatory requirements
D. Organizational goals

Answer: D

NEW QUESTION 848
- (Exam Topic 2)
A bank is experiencing an increasing incidence of customer identity theft. Which of the following is the BEST way to mitigate this risk?

A. Implement monitoring techniques.
B. Implement layered security.
C. Outsource to a local processor.
D. Conduct an awareness campaign.

Answer: B

NEW QUESTION 851
- (Exam Topic 2)
Which of the following is MOST important when defining controls?

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

Answer: C

NEW QUESTION 853
- (Exam Topic 2)
Which of the following is the MOST important consideration when selecting either a qualitative or quantitative risk analysis?

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

Answer: D

NEW QUESTION 857

- (Exam Topic 2)
When reporting risk assessment results to senior management, which of the following is MOST important to include to enable risk-based decision making?

A. Risk action plans and associated owners
B. Recent audit and self-assessment results
C. Potential losses compared to treatment cost
D. A list of assets exposed to the highest risk

Answer: A

NEW QUESTION 861
- (Exam Topic 2)
A risk practitioner shares the results of a vulnerability assessment for a critical business application with the business manager. Which of the following is the NEXT step?

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

Answer: B

NEW QUESTION 862
- (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 867
- (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 868
- (Exam Topic 2)
Which of the following is a detective control?

A. Limit check
B. Periodic access review
C. Access control software
D. Rerun procedures

Answer: B

NEW QUESTION 872
- (Exam Topic 2)
An organization plans to migrate sensitive information to a public cloud infrastructure. Which of the following is the GREATEST security risk in this scenario?

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

Answer: A

NEW QUESTION 875
- (Exam Topic 2)
Who should be responsible for strategic decisions on risk management?

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

Answer: B

NEW QUESTION 879
- (Exam Topic 2)
The PRIMARY basis for selecting a security control is:

A. to achieve the desired level of maturity.
B. the materiality of the risk.
C. the ability to mitigate risk.
D. the cost of the control.

Answer: C

NEW QUESTION 884
- (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 889
- (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 890
- (Exam Topic 2)
Which of the following resources is MOST helpful when creating a manageable set of IT risk scenarios?

A. Results of current and past risk assessments
B. Organizational strategy and objectives
C. Lessons learned from materialized risk scenarios
D. Internal and external audit findings

Answer: B

NEW QUESTION 895
- (Exam Topic 2)
Which of the following conditions presents the GREATEST risk to an application?

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

Answer: D

NEW QUESTION 896
.....

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