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

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

Answer: C

NEW QUESTION 4
- (Exam Topic 4)
Which of the following should be the GREATEST concern to a risk practitioner when process documentation is incomplete?

A. Inability to allocate resources efficiently
B. Inability to identify the risk owner
C. Inability to complete the risk register
D. Inability to identify process experts

Answer: B

NEW QUESTION 5
- (Exam Topic 4)
A failed IT system upgrade project has resulted in the corruption of an organization's asset inventory database. Which of the following controls BEST mitigates the impact of this incident?

A. Encryption
B. Authentication
C. Configuration
D. Backups

Answer: D

NEW QUESTION 6
- (Exam Topic 4)
Which of the following is the PRIMARY accountability for a control owner?

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

Answer: C

NEW QUESTION 7
- (Exam Topic 4)
An organization has decided to postpone the assessment and treatment of several risk scenarios because stakeholders are unavailable. As a result of this decision, the risk associated with these new entries has been;

A. mitigated
B. deferred

C. accepted.
D. transferred

Answer: C

NEW QUESTION 8
- (Exam Topic 4)
Which of the following is the BEST way to ensure data is properly sanitized while in cloud storage?

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

Answer: B

NEW QUESTION 9
- (Exam Topic 4)
An organization's business gap analysis reveals the need for a robust IT risk strategy. Which of the following should be the risk practitioner's PRIMARY consideration when participating in development of the new strategy?

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

Answer: C

NEW QUESTION 10
- (Exam Topic 4)
Which of the following would provide the MOST useful input when evaluating the appropriateness of risk responses?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 4)
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, program for all employees of the organization?

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

Answer: C

NEW QUESTION 13
- (Exam Topic 4)
Which of the following would provide the MOST reliable evidence of the effectiveness of security controls implemented for a web application?

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

Answer: A

NEW QUESTION 17
- (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 21
- (Exam Topic 4)
The MOST important measure of the effectiveness of risk management in project implementation is the percentage of projects:

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

Answer: A

NEW QUESTION 25
- (Exam Topic 4)
Risk appetite should be PRIMARILY driven by which of the following?

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

Answer: B

NEW QUESTION 28
- (Exam Topic 4)
An organization is considering outsourcing user administration controls tor a critical system. The potential vendor has offered to perform quarterly sett-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to me risk practitioner?

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

Answer: D

NEW QUESTION 30
- (Exam Topic 4)
Which of the following provides the MOST useful information for developing key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 32
- (Exam Topic 4)
A cote data center went offline abruptly for several hours affecting many transactions across multiple locations. Which of the to" owing would provide the MOST useful information to determine mitigating controls?

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

Answer: A

NEW QUESTION 33
- (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 (KRls)

Answer: C

NEW QUESTION 35
- (Exam Topic 4)
Which component of a software inventory BEST enables the identification and mitigation of known vulnerabilities?

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

Answer: A

NEW QUESTION 40

- (Exam Topic 4)
An organization has decided to implement a new Internet of Things (loT) solution. Which of the following should be done FIRST when addressing security concerns associated with this new technology?

A. Develop new loT risk scenarios.
B. Implement loT device monitoring software.
C. Introduce controls to the new threat environment.
D. Engage external security reviews.

Answer: A

NEW QUESTION 45
- (Exam Topic 4)
Which of the following should be the FIRST consideration when establishing a new risk governance program?

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

Answer: B

NEW QUESTION 49
- (Exam Topic 4)
Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

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

Answer: D

NEW QUESTION 53
- (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 58
- (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 59
- (Exam Topic 4)
Which of the following practices would be MOST effective in protecting personality identifiable information
(Ptl) from unauthorized access m a cloud environment?

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

Answer: B

NEW QUESTION 62
- (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 63
- (Exam Topic 4)
An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis Which of the following is the MOST important control to ensure the privacy of customer information?

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

Answer: C

NEW QUESTION 68
- (Exam Topic 4)
Which of the following is MOST important to determine when assessing the potential risk exposure of a loss event involving personal data?

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

Answer: C

NEW QUESTION 73
- (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 78
- (Exam Topic 4)
A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?

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

Answer: C

NEW QUESTION 81
- (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 84
- (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 89
- (Exam Topic 4)
Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

A. Incomplete end-user device inventory
B. Unsupported end-user applications

C. Incompatible end-user devices
D. Multiple end-user device models

Answer: A

NEW QUESTION 92
- (Exam Topic 4)
Which of the following is the BEST way to validate whether controls to reduce user device vulnerabilities have been implemented according to management's action plan?

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

Answer: B

NEW QUESTION 96
- (Exam Topic 4)
Which of the following is the PRIMARY purpose of creating and documenting control procedures?

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

Answer: D

NEW QUESTION 97
- (Exam Topic 4)
Which of the following is the BEST method to maintain a common view of IT risk within an organization?

A. Collecting data for IT risk assessment
B. Establishing and communicating the IT risk profile
C. Utilizing a balanced scorecard
D. Performing and publishing an IT risk analysis

Answer: C

NEW QUESTION 100
- (Exam Topic 4)
Which of the following provides the BEST assurance of the effectiveness of vendor security controls?

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

Answer: C

NEW QUESTION 103
- (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 108
- (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 110
- (Exam Topic 4)
A recent big data project has resulted in the creation of an application used to support important investment decisions. Which of the following should be of

GREATEST concern to the risk practitioner?

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

Answer: A

NEW QUESTION 113
- (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 114
- (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 115
- (Exam Topic 3)
An organization has implemented a preventive control to lock user accounts after three unsuccessful login attempts. This practice has been proven to be unproductive, and a change in the control threshold value has been recommended. Who should authorize changing this threshold?

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

Answer: D

NEW QUESTION 119
- (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 123
- (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 124
- (Exam Topic 3)
Which of the following provides the BEST evidence that a selected risk treatment plan is effective?

A. Identifying key risk indicators (KRIs)
B. Evaluating the return on investment (ROI)
C. Evaluating the residual risk level
D. Performing a cost-benefit analysis

Answer: D

NEW QUESTION 126
- (Exam Topic 3)
Which of the following is the BEST way to determine the potential organizational impact of emerging privacy regulations?

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

Answer: D

NEW QUESTION 129
- (Exam Topic 3)
Winch of the following can be concluded by analyzing the latest vulnerability report for the it infrastructure?

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

Answer: C

NEW QUESTION 134
- (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 137
- (Exam Topic 3)
Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?

A. Key risk indicators (KRIs)
B. Key management indicators (KMIs)
C. Key performance indicators (KPIs)
D. Key control indicators (KCIs)

Answer: D

NEW QUESTION 142
- (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 147
- (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 152
- (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 153
- (Exam Topic 3)
The PRIMARY benefit associated with key risk indicators (KRIs) is that they:

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

Answer: D

NEW QUESTION 154
- (Exam Topic 3)
Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

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

Answer: C

NEW QUESTION 155
- (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 158
- (Exam Topic 3)
Which of the following should be considered when selecting a risk response?

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

Answer: B

NEW QUESTION 162
- (Exam Topic 3)
Which of the following is the MOST appropriate key risk indicator (KRI) for backup media that is recycled monthly?

A. Time required for backup restoration testing
B. Change in size of data backed up
C. Successful completion of backup operations
D. Percentage of failed restore tests

Answer: D

NEW QUESTION 163
- (Exam Topic 3)
The PRIMARY purpose of using a framework for risk analysis is to:

A. improve accountability
B. improve consistency
C. help define risk tolerance
D. help develop risk scenarios.

Answer: B

NEW QUESTION 168
- (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 171
- (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 174
- (Exam Topic 3)
When developing a new risk register, a risk practitioner should focus on which of the following risk management activities?

A. Risk management strategy planning
B. Risk monitoring and control
C. Risk identification
D. Risk response planning

Answer: C

NEW QUESTION 179
- (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 180
- (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 182
- (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 183
- (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 184

- (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 186
- (Exam Topic 3)
Which of the following is the MOST appropriate action when a tolerance threshold is exceeded?

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

Answer: A

NEW QUESTION 187
- (Exam Topic 3)
Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

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

Answer: B

NEW QUESTION 191
- (Exam Topic 3)
An IT department originally planned to outsource the hosting of its data center at an overseas location to reduce operational expenses. After a risk assessment, the department has decided to keep the data center in-house. How should the risk treatment response be reflected in the risk register?

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

Answer: A

NEW QUESTION 194
- (Exam Topic 3)
Which of the following is the PRIMARY risk management responsibility of the second line of defense?

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

Answer: A

NEW QUESTION 197
- (Exam Topic 3)
Which of the following is MOST important when developing key risk indicators (KRIs)?

A. Alignment with regulatory requirements
B. Availability of qualitative data
C. Properly set thresholds
D. Alignment with industry benchmarks

Answer: C

NEW QUESTION 198
- (Exam Topic 3)
Which of the following BEST indicates the condition of a risk management program?

A. Number of risk register entries
B. Number of controls
C. Level of financial support
D. Amount of residual risk

Answer: D

NEW QUESTION 201
- (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 203
- (Exam Topic 3)
When of the following provides the MOST tenable evidence that a business process control is effective?

A. Demonstration that the control is operating as designed
B. A successful walk-through of the associated risk assessment
C. Management attestation that the control is operating effectively
D. Automated data indicating that risk has been reduced

Answer: C

NEW QUESTION 207
- (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 208
- (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 211
- (Exam Topic 3)
When performing a risk assessment of a new service to support a ewe Business process. which of the following should be done FRST10 ensure continuity of operations?

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

Answer: A

NEW QUESTION 216
- (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 220
- (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 222
- (Exam Topic 3)
While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

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

Answer: B

NEW QUESTION 226
- (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 229
- (Exam Topic 3)
An organization discovers significant vulnerabilities in a recently purchased commercial off-the-shelf software product which will not be corrected until the next release. Which of the following is the risk manager's BEST course of action?

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

Answer: C

NEW QUESTION 234
- (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 238
- (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 241
- (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 244
- (Exam Topic 3)
An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?

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

Answer: B

NEW QUESTION 246
- (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 251
- (Exam Topic 3)
Which of the following should be management's PRIMARY focus when key risk indicators (KRIs) begin to rapidly approach defined thresholds?

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

Answer: D

NEW QUESTION 253
- (Exam Topic 3)
Which of the following BEST indicates how well a web infrastructure protects critical information from an attacker?

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

Answer: D

NEW QUESTION 258
- (Exam Topic 3)
Which of the following is the PRIMARY role of a data custodian in the risk management process?

A. Performing periodic data reviews according to policy
B. Reporting and escalating data breaches to senior management
C. Being accountable for control design
D. Ensuring data is protected according to the classification

Answer: D

NEW QUESTION 259
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for risk related to IT infrastructure failure?

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

Answer: B

NEW QUESTION 264
- (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 267
- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 268
- (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 272
- (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 274
- (Exam Topic 3)
Which of the following is the MOST critical element to maximize the potential for a successful security implementation?

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

Answer: C

NEW QUESTION 278
- (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 279
- (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 280
- (Exam Topic 3)
Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?

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

Answer: B

NEW QUESTION 284

- (Exam Topic 3)
Which of the following provides the MOST useful information to determine risk exposure following control implementations?

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

Answer: C

NEW QUESTION 285
- (Exam Topic 3)
An organization is preparing to transfer a large number of customer service representatives to the sales department. Of the following, who is responsible for mitigating the risk associated with residual system access?

A. IT service desk manager
B. Sales manager
C. Customer service manager
D. Access control manager

Answer: D

NEW QUESTION 287
- (Exam Topic 3)
Which of the following would BEST assist in reconstructing the sequence of events following a security incident across multiple IT systems in the organization's network?

A. Network monitoring infrastructure
B. Centralized vulnerability management
C. Incident management process
D. Centralized log management

Answer: D

NEW QUESTION 291
- (Exam Topic 3)
Which of the following would present the MOST significant risk to an organization when updating the incident response plan?

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

Answer: D

NEW QUESTION 295
- (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 298
- (Exam Topic 3)
An organization is conducting a review of emerging risk. Which of the following is the BEST input for this exercise?

A. Audit reports
B. Industry benchmarks
C. Financial forecasts
D. Annual threat reports

Answer: B

NEW QUESTION 301
- (Exam Topic 3)
Which of the following is the GREATEST benefit for an organization with a strong risk awareness culture?

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

Answer: D

NEW QUESTION 302
- (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 307
- (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 308
- (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 309
- (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 310
- (Exam Topic 3)
When evaluating enterprise IT risk management it is MOST important to:

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

Answer: B

NEW QUESTION 314
- (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 317
- (Exam Topic 3)
Which of the following is a risk practitioner's BEST recommendation to address an organization's need to secure multiple systems with limited IT resources?

A. Apply available security patches.
B. Schedule a penetration test.
C. Conduct a business impact analysis (BIA)
D. Perform a vulnerability analysis.

Answer: C

NEW QUESTION 320
- (Exam Topic 3)
Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures?

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

Answer: D

NEW QUESTION 323
- (Exam Topic 3)
An organization moved its payroll system to a Software as a Service (SaaS) application. A new data privacy regulation stipulates that data can only be processed within the country where it is collected. Which of the following should be done FIRST when addressing this situation?

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

Answer: B

NEW QUESTION 327
- (Exam Topic 3)
What are the MOST essential attributes of an effective Key control indicator (KCI)?

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

Answer: B

NEW QUESTION 329
- (Exam Topic 3)
In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

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

Answer: B

NEW QUESTION 330
- (Exam Topic 3)
When updating the risk register after a risk assessment, which of the following is MOST important to include?

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

Answer: C

NEW QUESTION 335
- (Exam Topic 3)
When reporting on the performance of an organization's control environment including which of the following would BEST inform stakeholders risk decision-making?

A. The audit plan for the upcoming period
B. Spend to date on mitigating control implementation
C. A report of deficiencies noted during controls testing
D. A status report of control deployment

Answer: C

NEW QUESTION 337
- (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 342
- (Exam Topic 3)
Which of the following is MOST important to compare against the corporate risk profile?

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

Answer: D

NEW QUESTION 347
- (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 352
- (Exam Topic 3)
Which of the following would be MOST useful to senior management when determining an appropriate risk response?

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

Answer: A

NEW QUESTION 354
- (Exam Topic 3)
Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

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

Answer: B

NEW QUESTION 355
- (Exam Topic 3)
Which of the following issues should be of GREATEST concern when evaluating existing controls during a risk assessment?

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

Answer: B

NEW QUESTION 359
- (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 362
- (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 366
- (Exam Topic 3)
Which of the following approaches BEST identifies information systems control deficiencies?

A. Countermeasures analysis
B. Best practice assessment
C. Gap analysis
D. Risk assessment

Answer: C

NEW QUESTION 371
- (Exam Topic 3)
Which of the following would BEST indicate to senior management that IT processes are improving?

A. Changes in the number of intrusions detected
B. Changes in the number of security exceptions
C. Changes in the position in the maturity model
D. Changes to the structure of the risk register

Answer: B

NEW QUESTION 372
- (Exam Topic 3)
Which of The following is the MOST comprehensive input to the risk assessment process specific to the effects of system downtime?

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

Answer: C

NEW QUESTION 374
- (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 375
- (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 378
- (Exam Topic 3)
The PRIMARY benefit of using a maturity model is that it helps to evaluate the:

A. capability to implement new processes
B. evolution of process improvements
C. degree of compliance with policies and procedures
D. control requirements.

Answer: B

NEW QUESTION 379
- (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 380
- (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 382
- (Exam Topic 3)
An organization uses a vendor to destroy hard drives. Which of the following would BEST reduce the risk of data leakage?

A. Require the vendor to degauss the hard drives
B. Implement an encryption policy for the hard drives.
C. Require confirmation of destruction from the IT manager.
D. Use an accredited vendor to dispose of the hard drives.

Answer: B

NEW QUESTION 384
- (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 389
- (Exam Topic 3)
An organization has outsourced its billing function to an external service provider. Who should own the risk of customer data leakage caused by the service provider?

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

Answer: D

NEW QUESTION 394
- (Exam Topic 3)
Days before the realization of an acquisition, a data breach is discovered at the company to be acquired. For the accruing organization, this situation represents which of the following?

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

Answer: B

NEW QUESTION 397
- (Exam Topic 3)
An organization learns of a new ransomware attack affecting organizations worldwide. Which of the following should be done FIRST to reduce the likelihood of infection from the attack?

A. Identify systems that are vulnerable to being exploited by the attack.
B. Confirm with the antivirus solution vendor whether the next update will detect the attack.
C. Verify the data backup process and confirm which backups are the most recent ones available.

D. Obtain approval for funding to purchase a cyber insurance plan.

Answer: A

NEW QUESTION 402
- (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 407
- (Exam Topic 3)
A highly regulated organization acquired a medical technology startup company that processes sensitive personal information with weak data protection controls. Which of the following is the BEST way for the
acquiring company to reduce its risk while still enabling the flexibility needed by the startup company?

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

Answer: A

NEW QUESTION 412
- (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 413
- (Exam Topic 3)
A deficient control has been identified which could result in great harm to an organization should a low frequency threat event occur. When communicating the associated risk to senior management the risk practitioner should explain:

A. mitigation plans for threat events should be prepared in the current planning period.
B. this risk scenario is equivalent to more frequent but lower impact risk scenarios.
C. the current level of risk is within tolerance.
D. an increase in threat events could cause a loss sooner than anticipated.

Answer: A

NEW QUESTION 418
- (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 420
- (Exam Topic 3)
Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?

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

Answer: A

NEW QUESTION 422

- (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 423
- (Exam Topic 3)
All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

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

Answer: D

NEW QUESTION 424
- (Exam Topic 4)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

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

Answer: C

NEW QUESTION 428
- (Exam Topic 4)
Which of the following is the MOST important characteristic of a key risk indicator (KRI) to enable decision-making?

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

Answer: D

NEW QUESTION 432
- (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 437
- (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 438
- (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 440
- (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 441
- (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 445
- (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 447
- (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 448
- (Exam Topic 4)
An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

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

Answer: A

NEW QUESTION 449
- (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 451
- (Exam Topic 4)
An organization is analyzing the risk of shadow IT usage. Which of the following is the MOST important input into the assessment?

A. Business benefits of shadow IT
B. Application-related expresses
C. Classification of the data
D. Volume of data

Answer: A

NEW QUESTION 454
- (Exam Topic 4)
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

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

Answer: D

NEW QUESTION 457
- (Exam Topic 4)
Which of the following sources is MOST relevant to reference when updating security awareness training materials?

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

Answer: B

NEW QUESTION 462
- (Exam Topic 4)
A recent vulnerability assessment of a web-facing application revealed several weaknesses. Which of the following should be done NEXT to determine the risk exposure?

A. Code review
B. Penetration test
C. Gap assessment
D. Business impact analysis (BIA)

Answer: B

NEW QUESTION 463
- (Exam Topic 4)
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

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

Answer: D

NEW QUESTION 465
- (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 468
- (Exam Topic 4)
Which of the following provides the MOST comprehensive information when developing a risk profile for a system?

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

Answer: B

NEW QUESTION 470
- (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 473
- (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 477
- (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 481
- (Exam Topic 4)
When implementing an IT risk management program, which of the following is the BEST time to evaluate current control effectiveness?

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

Answer: B

NEW QUESTION 483
- (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 487
- (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 489
- (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 490

- (Exam Topic 4)
Following an acquisition, the acquiring company's risk practitioner has been asked to update the organization's IT risk profile What is the MOST important information to review from the acquired company to facilitate this task?

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

Answer: C

NEW QUESTION 494
- (Exam Topic 4)
Which of the following will BEST help to ensure key risk indicators (KRIs) provide value to risk owners?

A. Ongoing training
B. Timely notification
C. Return on investment (ROI)
D. Cost minimization

Answer: B

NEW QUESTION 498
- (Exam Topic 4)
Which of the following is the BEST key performance indicator (KPI) to measure how effectively risk management practices are embedded in the project management office (PMO)?

A. Percentage of projects with key risk accepted by the project steering committee
B. Reduction in risk policy noncompliance findings
C. Percentage of projects with developed controls on scope creep
D. Reduction in audits involving external risk consultants

Answer: C

NEW QUESTION 502
- (Exam Topic 4)
Which of the following is the MOST effective way 10 identify an application backdoor prior to implementation'?

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

Answer: B

NEW QUESTION 507
- (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 510
- (Exam Topic 4)
Which of the following contributes MOST to the effective implementation of risk responses?

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

Answer: A

NEW QUESTION 514
- (Exam Topic 4)
An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate tins risk?

A. Requiring the use of virtual private networks (VPNs)
B. Establishing a data classification policy
C. Conducting user awareness training

D. Requiring employee agreement of the acceptable use policy

Answer: C

NEW QUESTION 517
- (Exam Topic 4)
Which of the following would MOST likely require a risk practitioner to update the risk register?

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

Answer: C

NEW QUESTION 518
- (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 523
- (Exam Topic 4)
An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

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

Answer: D

NEW QUESTION 526
- (Exam Topic 4)
Which stakeholder is MOST important to include when defining a risk profile during me selection process for a new third party application'?

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

Answer: B

NEW QUESTION 528
- (Exam Topic 4)
An organization wants to grant remote access to a system containing sensitive data to an overseas third party. Which of the following should be of GREATEST concern to management?

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

Answer: C

NEW QUESTION 531
- (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 536
- (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 538
- (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 540
- (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 543
- (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 548
- (Exam Topic 4)
Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

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

Answer: C

NEW QUESTION 550
- (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 554
- (Exam Topic 4)
Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

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

Answer: A

NEW QUESTION 559
- (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 563
- (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 568
- (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 572
- (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 574
- (Exam Topic 4)
An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

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

Answer: B

NEW QUESTION 579
- (Exam Topic 4)
Which of the following is the BEST recommendation to address recent IT risk trends that indicate social engineering attempts are increasing in the organization?

A. Conduct a simulated phishing attack.
B. Update spam filters
C. Revise the acceptable use policy
D. Strengthen disciplinary procedures

Answer: A

NEW QUESTION 584
- (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 585
- (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 586
- (Exam Topic 4)
Which of the following is the MOST important consideration when communicating the risk associated with technology end-of-life to business owners?

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

Answer: A

NEW QUESTION 591
- (Exam Topic 4)
Which of the following is MOST helpful in identifying loss magnitude during risk analysis of a new system?

A. Recovery time objective (RTO)
B. Cost-benefit analysis
C. Business impact analysis (BIA)
D. Cyber insurance coverage

Answer: C

NEW QUESTION 592
- (Exam Topic 4)
An organization's recovery team is attempting to recover critical data backups following a major flood in its data center. However, key team members do not know exactly what steps should be taken to address this crisis. Which of the following is the MOST likely cause of this situation?

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

Answer: A

NEW QUESTION 595
- (Exam Topic 4)
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

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

Answer: A

NEW QUESTION 597
- (Exam Topic 4)
A control process has been implemented in response to a new regulatory requirement, but has significantly reduced productivity. Which of the following is the BEST way to resolve this concern?

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

Answer: C

NEW QUESTION 600
- (Exam Topic 4)
An organization plans to implement a new Software as a Service (SaaS) speech-to-text solution Which of the following is MOST important to mitigate risk associated with data privacy?

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

Answer: A

NEW QUESTION 602
- (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 607
- (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 609
- (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 610
- (Exam Topic 4)
Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

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

Answer: B

NEW QUESTION 613
- (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 616
- (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 621

- (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 625
- (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 628
- (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 633
- (Exam Topic 4)
An organization is considering the adoption of an aggressive business strategy to achieve desired growth From a risk management perspective what should the risk practitioner do NEXT?

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

Answer: A

NEW QUESTION 635
- (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 638
- (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 642
- (Exam Topic 4)
Which of the following is the PRIMARY reason to perform periodic vendor risk assessments?

A. To provide input to the organization's risk appetite
B. To monitor the vendor's control effectiveness
C. To verify the vendor's ongoing financial viability
D. To assess the vendor's risk mitigation plans

Answer: B

NEW QUESTION 646
- (Exam Topic 4)
In order to efficiently execute a risk response action plan, it is MOST important for the emergency response team members to understand:

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

Answer: D

NEW QUESTION 647
- (Exam Topic 4)
The cost of maintaining a control has grown to exceed the potential loss. Which of the following BEST describes this situation?

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

Answer: B

NEW QUESTION 649
- (Exam Topic 4)
Which of the following is the BEST method of creating risk awareness in an organization?

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

Answer: B

NEW QUESTION 654
- (Exam Topic 4)
Which of the following proposed benefits is MOST likely to influence senior management approval to reallocate budget for a new security initiative?

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

Answer: B

NEW QUESTION 656
- (Exam Topic 4)
Which of the following provides the MOST reliable evidence of a control's effectiveness?

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

Answer: D

NEW QUESTION 658
- (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 661
- (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 663
- (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 666
- (Exam Topic 4)
An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

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

Answer: A

NEW QUESTION 671
- (Exam Topic 4)
Before assigning sensitivity levels to information it is MOST important to:

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

Answer: B

NEW QUESTION 672
- (Exam Topic 4)
Which of the following is MOST important to include when reporting the effectiveness of risk management to senior management?

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

Answer: C

NEW QUESTION 673
- (Exam Topic 4)
Which of the following is the result of a realized risk scenario?

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

Answer: D

NEW QUESTION 675
- (Exam Topic 4)
Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

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

Answer: B

NEW QUESTION 676
- (Exam Topic 4)
Which of the following is MOST important to update when an organization's risk appetite changes?

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

D. Risk taxonomy

Answer: A

NEW QUESTION 680
- (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 682
- (Exam Topic 4)
Which key performance efficiency IKPI) BEST measures the effectiveness of an organization's disaster recovery program?

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

Answer: D

NEW QUESTION 687
- (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 688
- (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 691
- (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 696
- (Exam Topic 4)
Who should be responsible for determining which stakeholders need to be involved in the development of a risk scenario?

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

Answer: B

NEW QUESTION 698

- (Exam Topic 4)
An IT risk threat analysis is BEST used to establish

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

Answer: A

NEW QUESTION 699
- (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 701
- (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 704
- (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 707
- (Exam Topic 4)
After the implementation of internal of Things (IoT) devices, new risk scenarios were identified. What is the PRIMARY reason to report this information to risk owners?

A. To reevaluate continued use to IoT devices
B. The add new controls to mitigate the risk
C. The recommend changes to the IoT policy
D. To confirm the impact to the risk profile

Answer: D

NEW QUESTION 712
- (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 717
- (Exam Topic 4)
Which of the following would be of GREATEST concern regarding an organization's asset management?

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

Answer: D

NEW QUESTION 720
- (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 724
- (Exam Topic 4)
What should be the PRIMARY consideration related to data privacy protection when there are plans for a business initiative to make use of personal information?

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

Answer: D

NEW QUESTION 725
- (Exam Topic 4)
Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

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

Answer: A

NEW QUESTION 728
- (Exam Topic 4)
Which of the following should be the PRIMARY input to determine risk tolerance?

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

Answer: C

NEW QUESTION 731
- (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 735
- (Exam Topic 4)
After entering a large number of low-risk scenarios into the risk register, it is MOST important for the risk practitioner to:

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

Answer: D

NEW QUESTION 740
- (Exam Topic 4)
During a risk assessment, a risk practitioner learns that an IT risk factor is adequately mitigated by compensating controls in an associated business process. Which of the following would enable the MOST effective management of the residual risk?

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

Answer: A

NEW QUESTION 745
- (Exam Topic 4)
The BEST key performance indicator (KPI) to measure the effectiveness of the security patching process is the percentage of patches installed:

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

Answer: B

NEW QUESTION 750
- (Exam Topic 4)
Which of the following will BEST ensure that controls adequately support business goals and objectives?

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

Answer: A

NEW QUESTION 752
- (Exam Topic 4)
Which of the following would BEST mitigate the ongoing risk associated with operating system (OS) vulnerabilities?

A. Temporarily mitigate the OS vulnerabilities
B. Document and implement a patching process
C. Evaluate permanent fixes such as patches and upgrades
D. Identify the vulnerabilities and applicable OS patches

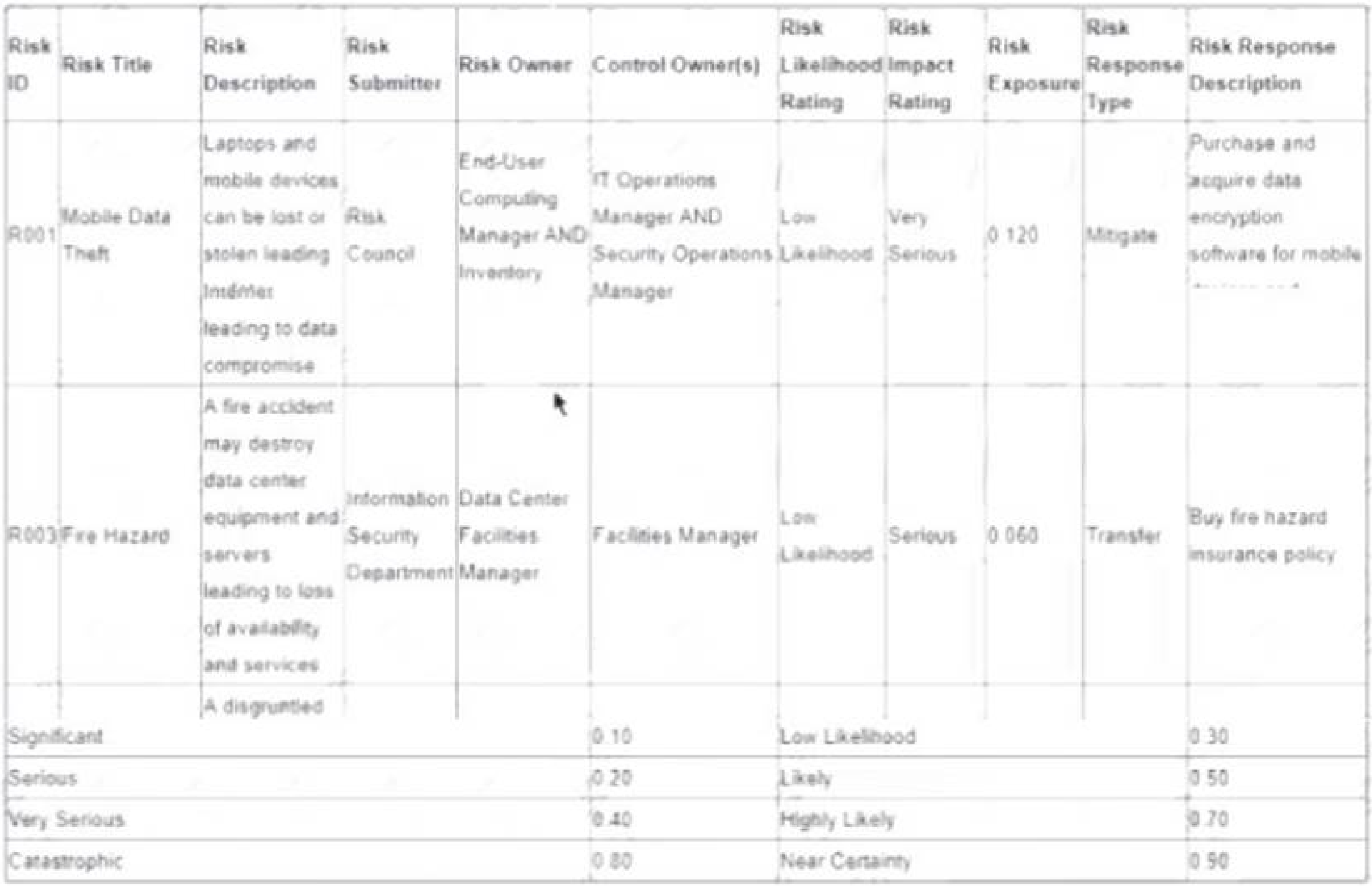
Answer: B

NEW QUESTION 753
- (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 755
- (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 Insider 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 759
- (Exam Topic 4)
Which of the following is MOST important for an organization to consider when developing its IT strategy?

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

Answer: C

NEW QUESTION 764
- (Exam Topic 4)
Which of the following is a risk practitioner's BEST course of action after identifying risk scenarios related to noncompliance with new industry regulations?

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

Answer: D

NEW QUESTION 769
- (Exam Topic 3)
Which of the following will be the GREATEST concern when assessing the risk profile of an organization?

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

Answer: A

NEW QUESTION 770
- (Exam Topic 3)
What information is MOST helpful to asset owners when classifying organizational assets for risk assessment?

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

Answer: A

NEW QUESTION 773
- (Exam Topic 3)
Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

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

Answer: A

NEW QUESTION 775
- (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 780
- (Exam Topic 3)
A risk practitioner has discovered a deficiency in a critical system that cannot be patched. Which of the following should be the risk practitioner's FIRST course of action?

A. Report the issue to internal audit.
B. Submit a request to change management.
C. Conduct a risk assessment.
D. Review the business impact assessment.

Answer: C

NEW QUESTION 781
- (Exam Topic 3)
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual
risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

A. Identify new risk entries to include in ERM.
B. Remove the risk entries from the ERM register.
C. Re-perform the risk assessment to confirm results.
D. Verify the adequacy of risk monitoring plans.

Answer: D

NEW QUESTION 784
- (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 788
- (Exam Topic 3)
Which of the following would BEST mitigate the risk associated with reputational damage from inappropriate use of social media sites by employees?

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

Answer: D

NEW QUESTION 792
- (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 796
- (Exam Topic 3)
When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

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

Answer: B

NEW QUESTION 799
- (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 804
- (Exam Topic 3)
Which element of an organization's risk register is MOST important to update following the commissioning of a new financial reporting system?

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

Answer: C

NEW QUESTION 808
- (Exam Topic 3)
A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

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

Answer: D

NEW QUESTION 810
- (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 811
- (Exam Topic 3)
What is the PRIMARY purpose of a business impact analysis (BIA)?

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

Answer: D

NEW QUESTION 813
- (Exam Topic 3)
Who should be PRIMARILY responsible for establishing an organization's IT risk culture?

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

Answer: B

NEW QUESTION 818
- (Exam Topic 3)
Which of the following practices BEST mitigates risk related to enterprise-wide ethical decision making in a multi-national organization?

A. Customized regional training on local laws and regulations
B. Policies requiring central reporting of potential procedure exceptions
C. Ongoing awareness training to support a common risk culture
D. Zero-tolerance policies for risk taking by middle-level managers

Answer: A

NEW QUESTION 822
- (Exam Topic 3)
An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

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

Answer: D

NEW QUESTION 825
- (Exam Topic 3)
Prudent business practice requires that risk appetite not exceed:

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

Answer: C

NEW QUESTION 830
- (Exam Topic 3)
Which of the following would be the GREATEST challenge when implementing a corporate risk framework for a global organization?

A. Privacy risk controls
B. Business continuity
C. Risk taxonomy
D. Management support

Answer: A

NEW QUESTION 833
- (Exam Topic 3)
Of the following, who is accountable for ensuing the effectiveness of a control to mitigate risk?

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

Answer: A

NEW QUESTION 835
- (Exam Topic 3)
Which of the following is the FIRST step in risk assessment?

A. Review risk governance
B. Asset identification

C. Identify risk factors
D. Inherent risk identification

Answer: B

NEW QUESTION 837
- (Exam Topic 3)
An organization's IT infrastructure is running end-of-life software that is not allowed without exception approval. Which of the following would provide the MOST helpful information to justify investing in updated software?

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

Answer: B

NEW QUESTION 841
- (Exam Topic 3)
A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

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

Answer: A

NEW QUESTION 846
- (Exam Topic 3)
Which of the following is the BEST course of action to help reduce the probability of an incident recurring?

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

Answer: B

NEW QUESTION 848
- (Exam Topic 3)
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 851
- (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 856
- (Exam Topic 3)
Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

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

Answer: C

NEW QUESTION 861
- (Exam Topic 3)
Which of the following is the BEST indicator of an effective IT security awareness program?

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

Answer: A

NEW QUESTION 864
- (Exam Topic 3)
Which of the following should be done FIRST when developing a data protection management plan?

A. Perform a cost-benefit analysis.
B. Identify critical data.
C. Establish a data inventory.
D. Conduct a risk analysis.

Answer: B

NEW QUESTION 865
- (Exam Topic 3)
An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?

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

Answer: C

NEW QUESTION 867
- (Exam Topic 3)
Which of the following poses the GREATEST risk to an organization's operations during a major it transformation?

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

Answer: D

NEW QUESTION 872
- (Exam Topic 3)
Which of the following BEST indicates the effectiveness of anti-malware software?

A. Number of staff hours lost due to malware attacks
B. Number of downtime hours in business critical servers
C. Number of patches made to anti-malware software
D. Number of successful attacks by malicious software

Answer: D

NEW QUESTION 875
- (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 880
- (Exam Topic 3)
Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

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

Answer: B

NEW QUESTION 883
- (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 887
- (Exam Topic 3)
The MAIN purpose of reviewing a control after implementation is to validate that the control:

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

Answer: A

NEW QUESTION 892
- (Exam Topic 3)
Which of the following BEST mitigates the risk of sensitive personal data leakage from a software development environment?

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

Answer: C

NEW QUESTION 893
- (Exam Topic 3)
A maturity model is MOST useful to an organization when it:

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

Answer: C

NEW QUESTION 898
- (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 899
......