Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (Exam Topic 3)
Which of the following would be a risk practitioner's BEST course of action when a project team has accepted a risk outside the established risk appetite?

A. Reject the risk acceptance and require mitigating controls.
B. Monitor the residual risk level of the accepted risk.
C. Escalate the risk decision to the project sponsor for review.
D. Document the risk decision in the project risk register.

Answer: B

NEW QUESTION 2
- (Exam Topic 3)
Which of the following BEST enables an organization to determine whether external emerging risk factors will impact the organization's risk profile?

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

Answer: D

NEW QUESTION 3
- (Exam Topic 3)
Which of the following is the MOST important topic to cover in a risk awareness training program for all staff?

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

Answer: C

NEW QUESTION 4
- (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 5
- (Exam Topic 3)
Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

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

Answer: C

NEW QUESTION 6
- (Exam Topic 3)
Which of We following is the MOST effective control to address the risk associated with compromising data privacy within the cloud?

A. Establish baseline security configurations with the cloud service provider.
B. Require the cloud prowler 10 disclose past data privacy breaches.
C. Ensure the cloud service provider performs an annual risk assessment.
D. Specify cloud service provider liability for data privacy breaches in the contract

Answer: D

NEW QUESTION 7
- (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 8
- (Exam Topic 3)
An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

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

Answer: B

NEW QUESTION 9
- (Exam Topic 3)
A risk practitioner identifies a database application that has been developed and implemented by the business independently of IT. Which of the following is the BEST course of action?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 3)
The MAIN reason for creating and maintaining a risk register is to:

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

Answer: D

NEW QUESTION 10
- (Exam Topic 3)
During implementation of an intrusion detection system (IDS) to monitor network traffic, a high number of alerts is reported. The risk practitioner should recommend to:

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

Answer: C

NEW QUESTION 11
- (Exam Topic 3)
Which of the following is MOST important to the integrity of a security log?

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

Answer: B

NEW QUESTION 12
- (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 14
- (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 17
- (Exam Topic 3)
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 21
- (Exam Topic 3)
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

Type	Scope	Completed By
External audit	Financial systems and processes	Third party
Internal audit	IT security risk management	Vendor
Vendor performance scorecard	Service level agreement compliance	Organization
Regulatory examination	Information security management program	Regulator

A. External audit
B. Internal audit
C. Vendor performance scorecard
D. Regulatory examination

Answer: A

NEW QUESTION 24
- (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 29
- (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 33
- (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 35
- (Exam Topic 3)
Which of the following BEST indicates that an organization has implemented IT performance requirements?

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

Answer: A

NEW QUESTION 40
- (Exam Topic 3)
Which of the following is the BEST control to minimize the risk associated with scope creep in software development?

A. An established process for project change management
B. Retention of test data and results for review purposes
C. Business managements review of functional requirements
D. Segregation between development, test, and production

Answer: A

NEW QUESTION 41
- (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 42
- (Exam Topic 3)
Which of the following is necessary to enable an IT risk register to be consolidated with the rest of the organization’s risk register?

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

Answer: A

NEW QUESTION 43
- (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: D

NEW QUESTION 47
- (Exam Topic 3)
Which of the following will help ensure the elective decision-making of an IT risk management committee?

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

Answer: D

NEW QUESTION 50
- (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 52
- (Exam Topic 3)
Which of the following would be a risk practitioner'$ BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

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

Answer: B

NEW QUESTION 55
- (Exam Topic 3)
An organization has an approved bring your own device (BYOD) policy. Which of the following would BEST mitigate the security risk associated with the inappropriate use of enterprise applications on the devices?

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

Answer: C

NEW QUESTION 59
- (Exam Topic 3)
The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

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

Answer: C

NEW QUESTION 61
- (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 64
- (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 67
- (Exam Topic 3)
The MOST important consideration when selecting a control to mitigate an identified risk is whether:

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

Answer: A

NEW QUESTION 72
- (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 76
- (Exam Topic 3)
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 77
- (Exam Topic 3)
The BEST reason to classify IT assets during a risk assessment is to determine the:

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

Answer: D

NEW QUESTION 82
- (Exam Topic 3)
An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

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

Answer: C

NEW QUESTION 87
- (Exam Topic 3)
Which of the following is the MOST important consideration when sharing risk management updates with executive management?

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

Answer: D

NEW QUESTION 89
- (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 91
- (Exam Topic 3)
Which of me following is MOST helpful to mitigate the risk associated with an application under development not meeting business objectives?

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

Answer: D

NEW QUESTION 94
- (Exam Topic 3)

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 95
- (Exam Topic 3)
Which of the following should be implemented to BEST mitigate the risk associated with infrastructure updates?

A. Role-specific technical training
B. Change management audit
C. Change control process
D. Risk assessment

Answer: C

NEW QUESTION 99
- (Exam Topic 3)
An IT control gap has been identified in a key process. Who would be the MOST appropriate owner of the risk associated with this gap?

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

Answer: A

NEW QUESTION 101
- (Exam Topic 3)
A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

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

Answer: D

NEW QUESTION 104
- (Exam Topic 3)
Which of the following is MOST important for senior management to review during an acquisition?

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

Answer: A

NEW QUESTION 106
- (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 108
- (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 113
- (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 115
- (Exam Topic 3)
Which of the following would BEST help an enterprise define and communicate its risk appetite?

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

Answer: C

NEW QUESTION 118
- (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 121
- (Exam Topic 3)
Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board"

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

Answer: C

NEW QUESTION 123
- (Exam Topic 3)
Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

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

Answer: B

NEW QUESTION 126
- (Exam Topic 3)
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 131
- (Exam Topic 3)
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 135
- (Exam Topic 3)
Which of the following is MOST important for an organization to update following a change in legislation requiring notification to individuals impacted by data breaches?

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

Answer: C

NEW QUESTION 137
- (Exam Topic 3)
The BEST metric to demonstrate that servers are configured securely is the total number of servers:

A. exceeding availability thresholds
B. experiencing hardware failures
C. exceeding current patching standards.
D. meeting the baseline for hardening.

Answer: D

NEW QUESTION 138
- (Exam Topic 3)
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 140
- (Exam Topic 3)
Which of the following will BEST help to ensure new IT policies address the enterprise's requirements?

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

Answer: B

NEW QUESTION 143
- (Exam Topic 3)
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 145
- (Exam Topic 3)
Which of the following is the BEST indication that key risk indicators (KRls) should be revised?

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

Answer: B

NEW QUESTION 149
- (Exam Topic 3)
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 154
- (Exam Topic 3)
Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

A. Organizational reporting process
B. Incident reporting procedures
C. Regularly scheduled audits
D. Incident management policy

Answer: A

NEW QUESTION 157
- (Exam Topic 3)
What is the PRIMARY reason an organization should include background checks on roles with elevated access to production as part of its hiring process?

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

Answer: C

NEW QUESTION 160
- (Exam Topic 3)
Which of the following is MOST important when developing risk scenarios?

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

Answer: D

NEW QUESTION 162
- (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 163
- (Exam Topic 3)
An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:

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

Answer: D

NEW QUESTION 167
- (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: B

NEW QUESTION 168

- (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 170
- (Exam Topic 3)
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 172
- (Exam Topic 3)
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 175
- (Exam Topic 3)
Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

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

Answer: A

NEW QUESTION 179
- (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: C

NEW QUESTION 181
- (Exam Topic 3)
Which of the following should a risk practitioner recommend FIRST when an increasing trend of risk events and subsequent losses has been identified?

A. Conduct root cause analyses for risk events.
B. Educate personnel on risk mitigation strategies.
C. Integrate the risk event and incident management processes.
D. Implement controls to prevent future risk events.

Answer: C

NEW QUESTION 183
- (Exam Topic 3)
An organization is implementing internet of Things (loT) technology to control temperature and lighting in its headquarters. Which of the following should be of GREATEST concern?

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

Answer: D

NEW QUESTION 188
- (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 192
- (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 193
- (Exam Topic 3)
Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

A. Perform a return on investment analysis.
B. Review the risk register and risk scenarios.
C. Calculate annualized loss expectancy of risk scenarios.
D. Raise the maturity of organizational risk management.

Answer: D

NEW QUESTION 194
- (Exam Topic 3)
Which of the following trends would cause the GREATEST concern regarding the effectiveness of an organization's user access control processes? An increase in the:

A. ratio of disabled to active user accounts.
B. percentage of users with multiple user accounts.
C. average number of access entitlements per user account.
D. average time between user transfers and access updates.

Answer: D

NEW QUESTION 196
- (Exam Topic 3)
The MOST important objective of information security controls is to:

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

Answer: C

NEW QUESTION 201
- (Exam Topic 3)
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 203
- (Exam Topic 3)
Which of the following MUST be updated to maintain an IT risk register?

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

Answer: C

NEW QUESTION 206
- (Exam Topic 3)
Using key risk indicators (KRIs) to illustrate changes in the risk profile PRIMARILY helps to:

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

Answer: A

NEW QUESTION 210
- (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 213
- (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 216
- (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 220
- (Exam Topic 3)
Which of the following is MOST helpful in providing an overview of an organization's risk management program?

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

Answer: C

NEW QUESTION 221
- (Exam Topic 3)
Which of the following represents a vulnerability?

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

Answer: C

NEW QUESTION 226

- (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 228
- (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 229
- (Exam Topic 3)
An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

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

Answer: C

NEW QUESTION 233
- (Exam Topic 3)
During a risk assessment, a key external technology supplier refuses to provide control design and effectiveness information, citing confidentiality concerns. What should the risk practitioner do NEXT?

A. Escalate the non-cooperation to management
B. Exclude applicable controls from the assessment.
C. Review the supplier's contractual obligations.
D. Request risk acceptance from the business process owner.

Answer: C

NEW QUESTION 234
- (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 238
- (Exam Topic 3)
Which of the following provides the MOST useful information when developing a risk profile for management approval?

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

Answer: A

NEW QUESTION 242
- (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 243
- (Exam Topic 3)
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 248
- (Exam Topic 3)
The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:

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

Answer: A

NEW QUESTION 252
- (Exam Topic 3)
While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

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

Answer: D

NEW QUESTION 256
- (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 259
- (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 263
- (Exam Topic 3)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an antivirus program?

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

Answer: A

NEW QUESTION 264
- (Exam Topic 3)
When formulating a social media policy lo address information leakage, which of the following is the MOST important concern to address?

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

Answer: A

NEW QUESTION 265
- (Exam Topic 3)
From a risk management perspective, the PRIMARY objective of using maturity models is to enable:

A. solution delivery.
B. resource utilization.
C. strategic alignment.
D. performance evaluation.

Answer: C

NEW QUESTION 270
- (Exam Topic 3)
An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

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

Answer: B

NEW QUESTION 275
- (Exam Topic 3)
A risk practitioner has become aware of production data being used in a test environment. Which of the following should be the practitioner's PRIMARY concern?

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

Answer: A

NEW QUESTION 278
- (Exam Topic 3)
An internal audit report reveals that not all IT application databases have encryption in place. Which of the following information would be MOST important for assessing the risk impact?

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

Answer: B

NEW QUESTION 281
- (Exam Topic 3)
A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

A. Identify changes in risk factors and initiate risk reviews.
B. Engage an external consultant to redesign the risk management process.
C. Outsource the process for updating the risk register.
D. Implement a process improvement and replace the old risk register.

Answer: A

NEW QUESTION 286
- (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 289
- (Exam Topic 3)
Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

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

Answer: D

NEW QUESTION 292
- (Exam Topic 3)
Which of the following is the STRONGEST indication an organization has ethics management issues?

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

Answer: A

NEW QUESTION 295
- (Exam Topic 3)
Which of the following will BEST support management reporting on risk?

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

Answer: C

NEW QUESTION 300
- (Exam Topic 3)
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 302
- (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 307
- (Exam Topic 3)
A violation of segregation of duties is when the same:

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

Answer: D

NEW QUESTION 312
- (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 314
- (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 315
- (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 317
- (Exam Topic 3)
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 319
- (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 320
- (Exam Topic 3)
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 321
- (Exam Topic 3)
As pan of business continuity planning, which of the following is MOST important to include m a business impact analysis (BIA)?

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

Answer: A

NEW QUESTION 323
- (Exam Topic 2)
An organization's internal audit department is considering the implementation of robotics process automation (RPA) to automate certain continuous auditing tasks. Who would own the risk associated with ineffective design of the software bots?

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

Answer: C

NEW QUESTION 324
- (Exam Topic 2)
An IT organization is replacing the customer relationship management (CRM) system. Who should own the risk associated with customer data leakage caused by insufficient IT security controls for the new system?

A. Chief information security officer
B. Business process owner
C. Chief risk officer
D. IT controls manager

Answer: B

NEW QUESTION 326
- (Exam Topic 2)
Which of the following BEST helps to identify significant events that could impact an organization? Vulnerability analysis

A. Control analysis
B. Scenario analysis
C. Heat map analysis

Answer: C

NEW QUESTION 328
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is aligned to business requirements?

A. Total cost to support the policy
B. Number of exceptions to the policy
C. Total cost of policy breaches
D. Number of inquiries regarding the policy

Answer: C

NEW QUESTION 330
- (Exam Topic 2)
Which of the following is MOST important for developing effective key risk indicators (KRIs)?

A. Engaging sponsorship by senior management
B. Utilizing data and resources internal to the organization
C. Including input from risk and business unit management
D. Developing in collaboration with internal audit

Answer: C

NEW QUESTION 331
- (Exam Topic 2)
A risk practitioner is reviewing a vendor contract and finds there is no clause to control privileged access to the organization's systems by vendor employees. Which of the following is the risk practitioner's BEST course of action?

A. Contact the control owner to determine if a gap in controls exists.
B. Add this concern to the risk register and highlight it for management review.
C. Report this concern to the contracts department for further action.
D. Document this concern as a threat and conduct an impact analysis.

Answer: D

NEW QUESTION 333
- (Exam Topic 2)
Which of the following is MOST important to enable well-informed cybersecurity risk decisions?

A. Determine and understand the risk rating of scenarios.
B. Conduct risk assessment peer reviews.
C. Identify roles and responsibilities for security controls.
D. Engage a third party to perform a risk assessment.

Answer: A

NEW QUESTION 338
- (Exam Topic 2)
An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?

A. Implement IT systems in alignment with business objectives.
B. Review metrics and key performance indicators (KPIs).
C. Review design documentation of IT systems.
D. Evaluate compliance with legal and regulatory requirements.

Answer: D

NEW QUESTION 341
- (Exam Topic 2)
Which of the following methods would BEST contribute to identifying obscure risk scenarios?

A. Brainstorming sessions
B. Control self-assessments
C. Vulnerability analysis
D. Monte Carlo analysis

Answer: A

NEW QUESTION 343
- (Exam Topic 2)
Which of the following would present the GREATEST challenge when assigning accountability for control ownership?

A. Weak governance structures
B. Senior management scrutiny
C. Complex regulatory environment
D. Unclear reporting relationships

Answer: D

NEW QUESTION 348
- (Exam Topic 2)
The PRIMARY basis for selecting a security control is:

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

Answer: C

NEW QUESTION 351
- (Exam Topic 2)
Which of the following is the BEST indication of the effectiveness of a business continuity program?

A. Business continuity tests are performed successfully and issues are addressed.
B. Business impact analyses are reviewed and updated in a timely manner.
C. Business continuity and disaster recovery plans are regularly updated.
D. Business units are familiar with the business continuity plans and process.

Answer: A

NEW QUESTION 355
- (Exam Topic 2)
Which of the following activities is PRIMARILY the responsibility of senior management?

A. Bottom-up identification of emerging risks
B. Categorization of risk scenarios against a standard taxonomy
C. Prioritization of risk scenarios based on severity
D. Review of external loss data

Answer: C

NEW QUESTION 360
- (Exam Topic 2)
Which of the following is MOST helpful in verifying that the implementation of a risk mitigation control has been completed as intended?

A. An updated risk register
B. Risk assessment results
C. Technical control validation
D. Control testing results

Answer: D

NEW QUESTION 364
- (Exam Topic 2)
Which of the following is the BEST way to ensure ongoing control effectiveness?

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

D. Obtaining management control attestations

Answer: C

NEW QUESTION 369
- (Exam Topic 2)
Which of the following is the BEST way to identify changes in the risk profile of an organization?

A. Monitor key risk indicators (KRIs).
B. Monitor key performance indicators (KPIs).
C. Interview the risk owner.
D. Conduct a gap analysis

Answer: D

NEW QUESTION 372
- (Exam Topic 2)
A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?

A. Recommend allowing the new usage based on prior approval.
B. Request a new third-party review.
C. Request revalidation of the original use case.
D. Assess the risk associated with the new use case.

Answer: D

NEW QUESTION 376
- (Exam Topic 2)
After identifying new risk events during a project, the project manager s NEXT step should be to:

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

Answer: B

NEW QUESTION 378
- (Exam Topic 2)
Which of the following should be the PRIMARY focus of an independent review of a risk management process?

A. Accuracy of risk tolerance levels
B. Consistency of risk process results
C. Participation of stakeholders
D. Maturity of the process

Answer: B

NEW QUESTION 379
- (Exam Topic 2)
The PRIMARY purpose of a maturity model is to compare the:

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

Answer: A

NEW QUESTION 380
- (Exam Topic 2)
Which of the following is MOST important to the effective monitoring of key risk indicators (KRIS)?

A. Updating the threat inventory with new threats
B. Automating log data analysis
C. Preventing the generation of false alerts
D. Determining threshold levels

Answer: D

NEW QUESTION 385
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to consider when determining the control requirements for data privacy arising from emerging technologies?

A. internal audit recommendations
B. Laws and regulations
C. Policies and procedures
D. Standards and frameworks

Answer: B

NEW QUESTION 390
- (Exam Topic 2)
From a risk management perspective, which of the following is the PRIMARY benefit of using automated system configuration validation tools?

A. Residual risk is reduced.
B. Staff costs are reduced.
C. Operational costs are reduced.
D. Inherent risk is reduced.

Answer: C

NEW QUESTION 391
- (Exam Topic 2)
Which of the following will BEST ensure that information security risk factors are mitigated when developing in-house applications?

A. Identify information security controls in the requirements analysis
B. Identify key risk indicators (KRIs) as process output.
C. Design key performance indicators (KPIs) for security in system specifications.
D. Include information security control specifications in business cases.

Answer: D

NEW QUESTION 393
- (Exam Topic 2)
When reporting risk assessment results to senior management, which of the following is MOST important to include to enable risk-based decision making?

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

Answer: A

NEW QUESTION 394
- (Exam Topic 2)
What should a risk practitioner do FIRST when vulnerability assessment results identify a weakness in an application?

A. Review regular control testing results.
B. Recommend a penetration test.
C. Assess the risk to determine mitigation needed.
D. Analyze key performance indicators (KPIs).

Answer: C

NEW QUESTION 398
- (Exam Topic 2)
Which of the following is MOST important when defining controls?

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

Answer: C

NEW QUESTION 403
- (Exam Topic 2)
Which of the following is the GREATEST concern associated with business end users developing their own applications on end user spreadsheets and database programs?

A. An IT project manager is not assigned to oversee development.
B. Controls are not applied to the applications.
C. There is a lack of technology recovery options.
D. The applications are not captured in the risk profile.

Answer: C

NEW QUESTION 405

- (Exam Topic 2)
Which of the following is MOST helpful to management when determining the resources needed to mitigate a risk?

A. An internal audit
B. A heat map
C. A business impact analysis (BIA)
D. A vulnerability report

Answer: C

NEW QUESTION 406
- (Exam Topic 2)
Whose risk tolerance matters MOST when making a risk decision?

A. Customers who would be affected by a breach
B. Auditors, regulators and standards organizations
C. The business process owner of the exposed assets
D. The information security manager

Answer: C

NEW QUESTION 410
- (Exam Topic 2)
Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

A. Risk tolerance
B. Risk appetite
C. Risk awareness
D. Risk policy

Answer: B

NEW QUESTION 415
- (Exam Topic 2)
An organization has received notification that it is a potential victim of a cybercrime that may have compromised sensitive customer data. What should be The FIRST course of action?

A. Invoke the incident response plan.
B. Determine the business impact.
C. Conduct a forensic investigation.
D. Invoke the business continuity plan (BCP).

Answer: A

NEW QUESTION 420
- (Exam Topic 2)
Which of the following is the PRIMARY objective for automating controls?

A. Improving control process efficiency
B. Facilitating continuous control monitoring
C. Complying with functional requirements
D. Reducing the need for audit reviews

Answer: A

NEW QUESTION 422
- (Exam Topic 2)
A risk practitioner is reviewing the status of an action plan to mitigate an emerging IT risk and finds the risk level has increased. The BEST course of action would be to:

A. implement the planned controls and accept the remaining risk.
B. suspend the current action plan in order to reassess the risk.
C. revise the action plan to include additional mitigating controls.
D. evaluate whether selected controls are still appropriate.

Answer: D

NEW QUESTION 426
- (Exam Topic 2)
Which of the following is the PRIMARY reason to establish the root cause of an IT security incident?

A. Update the risk register.
B. Assign responsibility and accountability for the incident.
C. Prepare a report for senior management.
D. Avoid recurrence of the incident.

Answer: D

NEW QUESTION 429
- (Exam Topic 2)
An organization is increasingly concerned about loss of sensitive data and asks the risk practitioner to assess the current risk level. Which of the following should the risk practitioner do FIRST?

A. Identify staff members who have access to the organization's sensitive data.
B. Identify locations where the organization's sensitive data is stored.
C. Identify risk scenarios and owners associated with possible data loss vectors.
D. Identify existing data loss controls and their levels of effectiveness.

Answer: D

NEW QUESTION 432
- (Exam Topic 2)
A control owner identifies that the organization's shared drive contains personally identifiable information (Pll) that can be accessed by all personnel. Which of the following is the MOST effective risk response?

A. Protect sensitive information with access controls.
B. Implement a data loss prevention (DLP) solution.
C. Re-communicate the data protection policy.
D. Implement a data encryption solution.

Answer: A

NEW QUESTION 435
- (Exam Topic 2)
Which of The following will BEST communicate the importance of risk mitigation initiatives to senior management?

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

Answer: A

NEW QUESTION 438
- (Exam Topic 2)
An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

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

Answer: B

NEW QUESTION 443
- (Exam Topic 2)
Which type of cloud computing deployment provides the consumer the GREATEST degree of control over the environment?

A. Community cloud
B. Private cloud
C. Hybrid cloud
D. Public cloud

Answer: B

NEW QUESTION 447
- (Exam Topic 2)
During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

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

Answer: A

NEW QUESTION 449
- (Exam Topic 2)
Which of the following is the BEST course of action when risk is found to be above the acceptable risk appetite?

A. Review risk tolerance levels
B. Maintain the current controls.
C. Analyze the effectiveness of controls.

D. Execute the risk response plan

Answer: D

NEW QUESTION 453
- (Exam Topic 2)
Which of the following is the BEST way to support communication of emerging risk?

A. Update residual risk levels to reflect the expected risk impact.
B. Adjust inherent risk levels upward.
C. Include it on the next enterprise risk committee agenda.
D. Include it in the risk register for ongoing monitoring.

Answer: D

NEW QUESTION 454
- (Exam Topic 2)
Which of the following is a detective control?

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

Answer: B

NEW QUESTION 456
- (Exam Topic 2)
Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

A. An internal audit
B. Security operations center review
C. Internal penetration testing
D. A third-party audit

Answer: D

NEW QUESTION 461
- (Exam Topic 2)
Which of the following is MOST commonly compared against the risk appetite?

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

Answer: D

NEW QUESTION 464
- (Exam Topic 2)
A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (Pll). Which of the following will MOST likely outcome for an organization affected by the new law?

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

Answer: B

NEW QUESTION 467
- (Exam Topic 2)
Which of the following is MOST important when discussing risk within an organization?

A. Adopting a common risk taxonomy
B. Using key performance indicators (KPIs)
C. Creating a risk communication policy
D. Using key risk indicators (KRIs)

Answer: A

NEW QUESTION 471
- (Exam Topic 2)
A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?

A. Reviewing access control lists
B. Authorizing user access requests
C. Performing user access recertification
D. Terminating inactive user access

Answer: B

NEW QUESTION 472
- (Exam Topic 2)
Which of the following is MOST helpful in identifying gaps between the current and desired state of the IT risk environment?

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

Answer: C

NEW QUESTION 475
- (Exam Topic 2)
Which of the following is the GREATEST concern when an organization uses a managed security service provider as a firewall administrator?

A. Exposure of log data
B. Lack of governance
C. Increased number of firewall rules
D. Lack of agreed-upon standards

Answer: B

NEW QUESTION 480
- (Exam Topic 2)
An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

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

Answer: B

NEW QUESTION 481
- (Exam Topic 2)
Which of the following is the BEST way to detect zero-day malware on an end user's workstation?

A. An antivirus program
B. Database activity monitoring
C. Firewall log monitoring
D. File integrity monitoring

Answer: C

NEW QUESTION 485
- (Exam Topic 2)
A business unit has decided to accept the risk of implementing an off-the-shelf, commercial software package that uses weak password controls. The BEST course of action would be to:

A. obtain management approval for policy exception.
B. develop an improved password software routine.
C. select another application with strong password controls.
D. continue the implementation with no changes.

Answer: B

NEW QUESTION 490
- (Exam Topic 2)
Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?

A. The KRIs' source data lacks integrity.
B. The KRIs are not automated.
C. The KRIs are not quantitative.
D. The KRIs do not allow for trend analysis.

Answer: A

NEW QUESTION 492

- (Exam Topic 2)
A new regulator/ requirement imposes severe fines for data leakage involving customers' personally identifiable information (PII). The risk practitioner has recommended avoiding the risk. Which of the following actions would BEST align with this recommendation?

A. Reduce retention periods for PII data.
B. Move PII to a highly-secured outsourced site.
C. Modify business processes to stop collecting PII.
D. Implement strong encryption for PII.

Answer: C

NEW QUESTION 493
- (Exam Topic 2)
An organization has decided to implement an emerging technology and incorporate the new capabilities into its strategic business plan. Business operations for the technology will be outsourced. What will be the risk practitioner's PRIMARY role during the change?

A. Managing third-party risk
B. Developing risk scenarios
C. Managing the threat landscape
D. Updating risk appetite

Answer: B

NEW QUESTION 495
- (Exam Topic 2)
A monthly payment report is generated from the enterprise resource planning (ERP) software to validate data against the old and new payroll systems. What is the BEST way to mitigate the risk associated with data integrity loss in the new payroll system after data migration?

A. Compare new system reports with functional requirements.
B. Compare encrypted data with checksums.
C. Compare results of user acceptance testing (UAT) with the testing criteria.
D. Compare processing output from both systems using the previous month's data.

Answer: D

NEW QUESTION 498
- (Exam Topic 2)
An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

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

Answer: D

NEW QUESTION 501
- (Exam Topic 2)
Which of the following would be MOST helpful to a risk owner when making risk-aware decisions?

A. Risk exposure expressed in business terms
B. Recommendations for risk response options
C. Resource requirements for risk responses
D. List of business areas affected by the risk

Answer: A

NEW QUESTION 503
- (Exam Topic 2)
The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:

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

Answer: B

NEW QUESTION 505
- (Exam Topic 2)
Which of the following MOST effectively limits the impact of a ransomware attack?

A. Cyber insurance
B. Cryptocurrency reserve
C. Data backups
D. End user training

Answer: C

NEW QUESTION 508
- (Exam Topic 2)
Which of the following is the GREATEST risk associated with the transition of a sensitive data backup solution from on-premise to a cloud service provider?

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

Answer: D

NEW QUESTION 509
- (Exam Topic 2)
Which of the following can be interpreted from a single data point on a risk heat map?

A. Risk tolerance
B. Risk magnitude
C. Risk response
D. Risk appetite

Answer: B

NEW QUESTION 512
- (Exam Topic 2)
Read" rights to application files in a controlled server environment should be approved by the:

A. business process owner.
B. database administrator.
C. chief information officer.
D. systems administrator.

Answer: A

NEW QUESTION 513
- (Exam Topic 2)
Which of the following BEST facilitates the development of effective IT risk scenarios?

A. Utilization of a cross-functional team
B. Participation by IT subject matter experts
C. Integration of contingency planning
D. Validation by senior management

Answer: A

NEW QUESTION 514
- (Exam Topic 2)
Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

A. Self-assessment questionnaires completed by management
B. Review of internal audit and third-party reports
C. Management review and sign-off on system documentation
D. First-hand direct observation of the controls in operation

Answer: B

NEW QUESTION 515
- (Exam Topic 2)
A risk practitioner learns that the organization s industry is experiencing a trend of rising security incidents. Which of the following is the BEST course of action?

A. Evaluate the relevance of the evolving threats.
B. Review past internal audit results.
C. Respond to organizational security threats.
D. Research industry published studies.

Answer: A

NEW QUESTION 519
- (Exam Topic 2)
The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

A. ensure policy and regulatory compliance.
B. assess the proliferation of new threats.
C. verify Internet firewall control settings.

D. identify vulnerabilities in the system.

Answer: C

NEW QUESTION 523
- (Exam Topic 2)
The risk associated with data loss from a website which contains sensitive customer information is BEST owned by:

A. the third-party website manager
B. the business process owner
C. IT security
D. the compliance manager

Answer: B

NEW QUESTION 526
- (Exam Topic 2)
An organization has introduced risk ownership to establish clear accountability for each process. To ensure effective risk ownership, it is MOST important that:

A. senior management has oversight of the process.
B. process ownership aligns with IT system ownership.
C. segregation of duties exists between risk and process owners.
D. risk owners have decision-making authority.

Answer: A

NEW QUESTION 530
- (Exam Topic 2)
Which of the following BEST measures the efficiency of an incident response process?

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

Answer: C

NEW QUESTION 531
- (Exam Topic 2)
An upward trend in which of the following metrics should be of MOST concern?

A. Number of business change management requests
B. Number of revisions to security policy
C. Number of security policy exceptions approved
D. Number of changes to firewall rules

Answer: C

NEW QUESTION 532
- (Exam Topic 2)
When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:

A. risk appetite.
B. security policies
C. process maps.
D. risk tolerance level

Answer: B

NEW QUESTION 534
- (Exam Topic 2)
When prioritizing risk response, management should FIRST:

A. evaluate the organization s ability and expertise to implement the solution.
B. evaluate the risk response of similar organizations.
C. address high risk factors that have efficient and effective solutions.
D. determine which risk factors have high remediation costs

Answer: C

NEW QUESTION 536
- (Exam Topic 2)
Within the three lines of defense model, the accountability for the system of internal control resides with:

A. the chief information officer (CIO).

B. the board of directors
C. enterprise risk management
D. the risk practitioner

Answer: B

NEW QUESTION 539
- (Exam Topic 2)
Which of The following is the MOST relevant information to include in a risk management strategy?

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

Answer: D

NEW QUESTION 541
- (Exam Topic 2)
A control owner has completed a year-long project To strengthen existing controls. It is MOST important for the risk practitioner to:

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

Answer: A

NEW QUESTION 542
- (Exam Topic 2)
A risk practitioner has learned that an effort to implement a risk mitigation action plan has stalled due to lack of funding. The risk practitioner should report that the associated risk has been:

A. mitigated
B. accepted
C. avoided
D. deferred

Answer: B

NEW QUESTION 546
- (Exam Topic 2)
An organization has identified that terminated employee accounts are not disabled or deleted within the time required by corporate policy. Unsure of the reason, the organization has decided to monitor the situation for three months to obtain more information. As a result of this decision, the risk has been:

A. avoided.
B. accepted.
C. mitigated.
D. transferred.

Answer: B

NEW QUESTION 548
- (Exam Topic 1)
A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:

A. communication
B. identification.
C. treatment.
D. assessment.

Answer: D

NEW QUESTION 550
- (Exam Topic 1)
The analysis of which of the following will BEST help validate whether suspicious network activity is malicious?

A. Logs and system events
B. Intrusion detection system (IDS) rules
C. Vulnerability assessment reports
D. Penetration test reports

Answer: B

NEW QUESTION 552

- (Exam Topic 1)
Which of the following elements of a risk register is MOST likely to change as a result of change in management's risk appetite?

A. Key risk indicator (KRI) thresholds
B. Inherent risk
C. Risk likelihood and impact
D. Risk velocity

Answer: A

NEW QUESTION 556
- (Exam Topic 1)
An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?

A. Invoke the disaster recovery plan during an incident.
B. Prepare a cost-benefit analysis of alternatives available
C. Implement redundant infrastructure for the application.
D. Reduce the recovery time by strengthening the response team.

Answer: C

NEW QUESTION 557
- (Exam Topic 3)
Which of the following should be the GREATEST concern for an organization that uses open source software applications?

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

Answer: A

NEW QUESTION 560
- (Exam Topic 3)
Which of the following would be MOST helpful to an information security management team when allocating resources to mitigate exposures?

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

Answer: C

NEW QUESTION 562
- (Exam Topic 3)
To reduce costs, an organization is combining the second and third tines of defense in a new department that reports to a recently appointed C-level executive. Which of the following is the GREATEST concern with this situation?

A. The risk governance approach of the second and third lines of defense may differ.
B. The independence of the internal third line of defense may be compromised.
C. Cost reductions may negatively impact the productivity of other departments.
D. The new structure is not aligned to the organization's internal control framework.

Answer: B

NEW QUESTION 566
- (Exam Topic 3)
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 568
- (Exam Topic 3)
The PRIMARY reason to have risk owners assigned to entries in the risk register is to ensure:

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

Answer: A

NEW QUESTION 572
- (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 573
- (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 578
- (Exam Topic 3)
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 579
- (Exam Topic 3)
Which of the following should be the PRIMARY focus of an IT risk awareness program?

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

Answer: B

NEW QUESTION 583
- (Exam Topic 3)
Which of the following is the MOST important consideration for protecting data assets m a Business application system?

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

Answer: A

NEW QUESTION 587
- (Exam Topic 3)
Which of the following is PRIMARILY a risk management responsibly of the first line of defense?

A. Implementing risk treatment plans
B. Validating the status of risk mitigation efforts
C. Establishing risk policies and standards
D. Conducting independent reviews of risk assessment results

Answer: C

NEW QUESTION 588
- (Exam Topic 3)
Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

A. Updating the risk register to include the risk mitigation plan
B. Determining processes for monitoring the effectiveness of the controls

C. Ensuring that control design reduces risk to an acceptable level
D. Confirming to management the controls reduce the likelihood of the risk

Answer: A

NEW QUESTION 590
- (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 595
- (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 596
- (Exam Topic 3)
Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

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

Answer: A

NEW QUESTION 601
- (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 605
- (Exam Topic 3)
Which of the following is the MOST important objective of an enterprise risk management (ERM) program?

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

Answer: B

NEW QUESTION 608
- (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 610
- (Exam Topic 3)
Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:

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

Answer: C

NEW QUESTION 613
- (Exam Topic 3)
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 617
- (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 619
- (Exam Topic 3)
Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

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

Answer: B

NEW QUESTION 624
- (Exam Topic 3)
Which of the following is the BEST way to mitigate the risk to IT infrastructure availability?

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

Answer: A

NEW QUESTION 626
- (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 628
- (Exam Topic 2)
Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?

A. Trends in IT resource usage
B. Trends in IT maintenance costs
C. Increased resource availability
D. Increased number of incidents

Answer: A

NEW QUESTION 629

- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of a control action plan's implementation?

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

Answer: B

NEW QUESTION 632
- (Exam Topic 2)
An organization is making significant changes to an application. At what point should the application risk profile be updated?

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

Answer: D

NEW QUESTION 635
- (Exam Topic 2)
What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

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

Answer: B

NEW QUESTION 636
- (Exam Topic 2)
Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

A. Self-assessment questionnaires completed by management
B. Review of internal audit and third-party reports
C. Management review and sign-off on system documentation
D. First-hand direct observation of the controls in operation

Answer: D

NEW QUESTION 639
- (Exam Topic 2)
Which of the following is the BEST way to determine software license compliance?

A. List non-compliant systems in the risk register.
B. Conduct periodic compliance reviews.
C. Review whistlebtower reports of noncompliance.
D. Monitor user software download activity.

Answer: B

NEW QUESTION 640
- (Exam Topic 2)
A maturity model will BEST indicate:

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

Answer: B

NEW QUESTION 645
- (Exam Topic 2)
During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?

A. Implement compensating controls to reduce residual risk
B. Escalate the issue to senior management
C. Discuss risk mitigation options with the risk owner.
D. Certify the control after documenting the concern.

Answer: A

NEW QUESTION 648
- (Exam Topic 2)
Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

A. Providing oversight of risk management processes
B. Implementing processes to detect and deter fraud
C. Ensuring that risk and control assessments consider fraud
D. Monitoring the results of actions taken to mitigate fraud

Answer: B

NEW QUESTION 650
- (Exam Topic 2)
Before implementing instant messaging within an organization using a public solution, which of the following should be in place to mitigate data leakage risk?

A. A data extraction tool
B. An access control list
C. An intrusion detection system (IDS)
D. An acceptable usage policy

Answer: D

NEW QUESTION 655
- (Exam Topic 2)
Which of the following should be a risk practitioner's MOST important consideration when developing IT risk scenarios?

A. The impact of controls on the efficiency of the business in delivering services
B. Linkage of identified risk scenarios with enterprise risk management
C. Potential threats and vulnerabilities that may have an impact on the business
D. Results of network vulnerability scanning and penetration testing

Answer: C

NEW QUESTION 660
- (Exam Topic 2)
An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?

A. Classification of the data
B. Type of device
C. Remote management capabilities
D. Volume of data

Answer: A

NEW QUESTION 661
- (Exam Topic 2)
Which of the following would be MOST beneficial as a key risk indicator (KRI)?

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

Answer: D

NEW QUESTION 666
- (Exam Topic 2)
Which of the following provides the MOST helpful information in identifying risk in an organization?

A. Risk registers
B. Risk analysis
C. Risk scenarios
D. Risk responses

Answer: C

NEW QUESTION 669
- (Exam Topic 2)
A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration when establishing a contingency plan and an alternate processing site?

A. The alternative site is a hot site with equipment ready to resume processing immediately.
B. The contingency plan provides for backup media to be taken to the alternative site.
C. The contingency plan for high priority applications does not involve a shared cold site.
D. The alternative site does not reside on the same fault to matter how the distance apart.

Answer: B

NEW QUESTION 671
- (Exam Topic 2)
Which of the following is MOST important to include in a Software as a Service (SaaS) vendor agreement?

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

Answer: B

NEW QUESTION 674
- (Exam Topic 2)
Which of the following is the GREATEST concern associated with the transmission of healthcare data across the internet?

A. Unencrypted data
B. Lack of redundant circuits
C. Low bandwidth connections
D. Data integrity

Answer: A

NEW QUESTION 676
- (Exam Topic 2)
Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?

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

Answer: D

NEW QUESTION 677
- (Exam Topic 1)
An organization delegates its data processing to the internal IT team to manage information through its applications. Which of the following is the role of the internal IT team in this situation?

A. Data controllers
B. Data processors
C. Data custodians
D. Data owners

Answer: B

NEW QUESTION 681
- (Exam Topic 1)
Which of the following is the MOST important factor affecting risk management in an organization?

A. The risk manager's expertise
B. Regulatory requirements
C. Board of directors' expertise
D. The organization's culture

Answer: D

NEW QUESTION 682
- (Exam Topic 1)
Which of the following will BEST mitigate the risk associated with IT and business misalignment?

A. Establishing business key performance indicators (KPIs)
B. Introducing an established framework for IT architecture
C. Establishing key risk indicators (KRIs)
D. Involving the business process owner in IT strategy

Answer: D

NEW QUESTION 683
- (Exam Topic 1)
The BEST way to justify the risk mitigation actions recommended in a risk assessment would be to:

A. align with audit results.
B. benchmark with competitor s actions.

C. reference best practice.
D. focus on the business drivers

Answer: D

NEW QUESTION 684
- (Exam Topic 1)
Which of the following is MOST helpful in identifying new risk exposures due to changes in the business environment?

A. Standard operating procedures
B. SWOT analysis
C. Industry benchmarking
D. Control gap analysis

Answer: B

NEW QUESTION 687
- (Exam Topic 1)
Which of the following is the BEST way to validate the results of a vulnerability assessment?

A. Perform a penetration test.
B. Review security logs.
C. Conduct a threat analysis.
D. Perform a root cause analysis.

Answer: A

NEW QUESTION 688
- (Exam Topic 1)
Which of the following would be MOST important for a risk practitioner to provide to the internal audit department during the audit planning process?

A. Closed management action plans from the previous audit
B. Annual risk assessment results
C. An updated vulnerability management report
D. A list of identified generic risk scenarios

Answer: A

NEW QUESTION 691
- (Exam Topic 1)
A business unit is updating a risk register with assessment results for a key project. Which of the following is MOST important to capture in the register?

A. The team that performed the risk assessment
B. An assigned risk manager to provide oversight
C. Action plans to address risk scenarios requiring treatment
D. The methodology used to perform the risk assessment

Answer: B

NEW QUESTION 693
- (Exam Topic 1)
An unauthorized individual has socially engineered entry into an organization's secured physical premises. Which of the following is the BEST way to prevent future occurrences?

A. Employ security guards.
B. Conduct security awareness training.
C. Install security cameras.
D. Require security access badges.

Answer: B

NEW QUESTION 696
- (Exam Topic 1)
Which of the following is the BEST approach to use when creating a comprehensive set of IT risk scenarios?

A. Derive scenarios from IT risk policies and standards.
B. Map scenarios to a recognized risk management framework.
C. Gather scenarios from senior management.
D. Benchmark scenarios against industry peers.

Answer: A

NEW QUESTION 697
- (Exam Topic 1)
An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?

A. Perform a risk assessment
B. Disable user access.
C. Develop an access control policy.
D. Perform root cause analysis.

Answer: B

NEW QUESTION 698
- (Exam Topic 1)
Which of the following is MOST critical when designing controls?

A. Involvement of internal audit
B. Involvement of process owner
C. Quantitative impact of the risk
D. Identification of key risk indicators

Answer: B

NEW QUESTION 703
- (Exam Topic 1)
A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

A. Document the finding in the risk register.
B. Invoke the incident response plan.
C. Re-evaluate key risk indicators.
D. Modify the design of the control.

Answer: A

NEW QUESTION 707
- (Exam Topic 1)
IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would
be MOST helpful?

A. IT risk register
B. List of key risk indicators
C. Internal audit reports
D. List of approved projects

Answer: A

NEW QUESTION 710
- (Exam Topic 1)
Which of the following is the FIRST step in managing the security risk associated with wearable technology in the workplace?

A. Identify the potential risk.
B. Monitor employee usage.
C. Assess the potential risk.
D. Develop risk awareness training.

Answer: A

NEW QUESTION 711
- (Exam Topic 1)
Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?

A. Assess the vulnerability management process.
B. Conduct a control serf-assessment.
C. Conduct a vulnerability assessment.
D. Reassess the inherent risk of the target.

Answer: A

NEW QUESTION 715
- (Exam Topic 1)
An organization has outsourced its IT security operations to a third party. Who is ULTIMATELY accountable
for the risk associated with the outsourced operations?

A. The third party s management
B. The organization's management
C. The control operators at the third party
D. The organization's vendor management office

Answer: B

NEW QUESTION 718
- (Exam Topic 1)
Which of the following activities would BEST contribute to promoting an organization-wide risk-aware culture?

A. Performing a benchmark analysis and evaluating gaps
B. Conducting risk assessments and implementing controls
C. Communicating components of risk and their acceptable levels
D. Participating in peer reviews and implementing best practices

Answer: C

NEW QUESTION 721
- (Exam Topic 1)
Whether the results of risk analyses should be presented in quantitative or qualitative terms should be based PRIMARILY on the:

A. requirements of management.
B. specific risk analysis framework being used.
C. organizational risk tolerance
D. results of the risk assessment.

Answer: A

NEW QUESTION 724
- (Exam Topic 1)
Which of the following would MOST effectively enable a business operations manager to identify events exceeding risk thresholds?

A. Continuous monitoring
B. A control self-assessment
C. Transaction logging
D. Benchmarking against peers

Answer: A

NEW QUESTION 729
- (Exam Topic 1)
Which of the following is the BEST way to determine the ongoing efficiency of control processes?

A. Perform annual risk assessments.
B. Interview process owners.
C. Review the risk register.
D. Analyze key performance indicators (KPIs).

Answer: D

NEW QUESTION 733
- (Exam Topic 1)
The head of a business operations department asks to review the entire IT risk register. Which of the following would be the risk manager s BEST approach to this request before sharing the register?

A. Escalate to senior management
B. Require a nondisclosure agreement.
C. Sanitize portions of the register
D. Determine the purpose of the request

Answer: D

NEW QUESTION 736
- (Exam Topic 1)
Who should be accountable for ensuring effective cybersecurity controls are established?

A. Risk owner
B. Security management function
C. IT management
D. Enterprise risk function

Answer: B

NEW QUESTION 738
- (Exam Topic 1)
Which of the following would BEST provide early warning of a high-risk condition?

A. Risk register
B. Risk assessment
C. Key risk indicator (KRI)
D. Key performance indicator (KPI)

Answer:

C

NEW QUESTION 740
- (Exam Topic 1)
Which of the following is MOST effective against external threats to an organizations confidential information?

A. Single sign-on
B. Data integrity checking
C. Strong authentication
D. Intrusion detection system

Answer: C

NEW QUESTION 743
- (Exam Topic 1)
Which of the following is the MOST important outcome of reviewing the risk management process?

A. Assuring the risk profile supports the IT objectives
B. Improving the competencies of employees who performed the review
C. Determining what changes should be nude to IS policies to reduce risk
D. Determining that procedures used in risk assessment are appropriate

Answer: A

NEW QUESTION 746
- (Exam Topic 1)
Which of the following should be the risk practitioner s PRIMARY focus when determining whether controls are adequate to mitigate risk?

A. Sensitivity analysis
B. Level of residual risk
C. Cost-benefit analysis
D. Risk appetite

Answer: C

NEW QUESTION 751
- (Exam Topic 1)
Which of the following is the MOST effective key performance indicator (KPI) for change management?

A. Percentage of changes with a fallback plan
B. Number of changes implemented
C. Percentage of successful changes
D. Average time required to implement a change

Answer: C

NEW QUESTION 753
- (Exam Topic 1)
Which of the following would BEST help to ensure that suspicious network activity is identified?

A. Analyzing intrusion detection system (IDS) logs
B. Analyzing server logs
C. Using a third-party monitoring provider
D. Coordinating events with appropriate agencies

Answer: A

NEW QUESTION 754
- (Exam Topic 1)
Which of the following is the BEST metric to demonstrate the effectiveness of an organization's change management process?

A. Increase in the frequency of changes
B. Percent of unauthorized changes
C. Increase in the number of emergency changes
D. Average time to complete changes

Answer: B

NEW QUESTION 756
- (Exam Topic 1)
Which of the following would BEST ensure that identified risk scenarios are addressed?

A. Reviewing the implementation of the risk response
B. Creating a separate risk register for key business units
C. Performing real-time monitoring of threats
D. Performing regular risk control self-assessments

Answer: C

NEW QUESTION 761
- (Exam Topic 1)
Which of the following BEST provides an early warning that network access of terminated employees is not being revoked in accordance with the service level agreement (SLA)?

A. Updating multi-factor authentication
B. Monitoring key access control performance indicators
C. Analyzing access control logs for suspicious activity
D. Revising the service level agreement (SLA)

Answer: B

NEW QUESTION 765
- (Exam Topic 1)
Which of the following is the MOST useful indicator to measure the efficiency of an identity and access management process?

A. Number of tickets for provisioning new accounts
B. Average time to provision user accounts
C. Password reset volume per month
D. Average account lockout time

Answer: C

NEW QUESTION 766
- (Exam Topic 1)
A risk assessment has identified that an organization may not be in compliance with industry regulations. The BEST course of action would be to:

A. conduct a gap analysis against compliance criteria.
B. identify necessary controls to ensure compliance.
C. modify internal assurance activities to include control validation.
D. collaborate with management to meet compliance requirements.

Answer: A

NEW QUESTION 767
- (Exam Topic 1)
During an IT risk scenario review session, business executives question why they have been assigned ownership of IT-related risk scenarios. They feel IT risk is technical in nature and therefore should be owned by IT. Which of the following is the BEST way for the risk practitioner to address these concerns?

A. Describe IT risk scenarios in terms of business risk.
B. Recommend the formation of an executive risk council to oversee IT risk.
C. Provide an estimate of IT system downtime if IT risk materializes.
D. Educate business executives on IT risk concepts.

Answer: A

NEW QUESTION 771
- (Exam Topic 1)
Which of the following roles would provide the MOST important input when identifying IT risk scenarios?

A. Information security managers
B. Internal auditors
C. Business process owners
D. Operational risk managers

Answer: C

NEW QUESTION 775
- (Exam Topic 1)
Which of the following would provide the BEST guidance when selecting an appropriate risk treatment plan?

A. Risk mitigation budget
B. Business Impact analysis
C. Cost-benefit analysis
D. Return on investment

Answer: C

NEW QUESTION 779
- (Exam Topic 1)
An organization has procured a managed hosting service and just discovered the location is likely to be flooded every 20 years. Of the following, who should be notified of this new information FIRST.

A. The risk owner who also owns the business service enabled by this infrastructure
B. The data center manager who is also employed under the managed hosting services contract
C. The site manager who is required to provide annual risk assessments under the contract
D. The chief information officer (CIO) who is responsible for the hosted services

Answer: A

NEW QUESTION 782
- (Exam Topic 1)
A web-based service provider with a low risk appetite for system outages is reviewing its current risk profile for online security. Which of the following observations would be MOST relevant to escalate to senior management?

A. An increase in attempted distributed denial of service (DDoS) attacks
B. An increase in attempted website phishing attacks
C. A decrease in achievement of service level agreements (SLAs)
D. A decrease in remediated web security vulnerabilities

Answer: A

NEW QUESTION 787
- (Exam Topic 1)
During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall. Which of the following controls has MOST likely been compromised?

A. Data validation
B. Identification
C. Authentication
D. Data integrity

Answer: C

NEW QUESTION 789
- (Exam Topic 1)
Which of the following should be the PRIMARY objective of promoting a risk-aware culture within an organization?

A. Better understanding of the risk appetite
B. Improving audit results
C. Enabling risk-based decision making
D. Increasing process control efficiencies

Answer: C

NEW QUESTION 790
- (Exam Topic 1)
Which of the following is a PRIMARY benefit of engaging the risk owner during the risk assessment process?

A. Identification of controls gaps that may lead to noncompliance
B. Prioritization of risk action plans across departments
C. Early detection of emerging threats
D. Accurate measurement of loss impact

Answer: D

NEW QUESTION 793
- (Exam Topic 1)
An effective control environment is BEST indicated by controls that:

A. minimize senior management's risk tolerance.
B. manage risk within the organization's risk appetite.
C. reduce the thresholds of key risk indicators (KRIs).
D. are cost-effective to implement

Answer: B

NEW QUESTION 795
- (Exam Topic 1)
A global organization is considering the acquisition of a competitor. Senior management has requested a review of the overall risk profile from the targeted organization. Which of the following components of this review would provide the MOST useful information?

A. Risk appetite statement
B. Enterprise risk management framework
C. Risk management policies
D. Risk register

Answer: D

NEW QUESTION 797
- (Exam Topic 1)
An organization that has been the subject of multiple social engineering attacks is developing a risk awareness program. The PRIMARY goal of this program should be to:

A. reduce the risk to an acceptable level.
B. communicate the consequences for violations.
C. implement industry best practices.
D. reduce the organization's risk appetite

Answer: B

NEW QUESTION 802
- (Exam Topic 1)
An organization is planning to engage a cloud-based service provider for some of its data-intensive business processes. Which of the following is MOST important to help define the IT risk associated with this outsourcing activity?

A. Service level agreement
B. Customer service reviews
C. Scope of services provided
D. Right to audit the provider

Answer: D

NEW QUESTION 805
- (Exam Topic 1)
Which of the following provides the BEST evidence of the effectiveness of an organization's account provisioning process?

A. User provisioning
B. Role-based access controls
C. Security log monitoring
D. Entitlement reviews

Answer: D

NEW QUESTION 810
- (Exam Topic 1)
Calculation of the recovery time objective (RTO) is necessary to determine the:

A. time required to restore files.
B. point of synchronization
C. priority of restoration.
D. annual loss expectancy (ALE).

Answer: A

NEW QUESTION 815
- (Exam Topic 1)
The PRIMARY reason a risk practitioner would be interested in an internal audit report is to:

A. plan awareness programs for business managers.
B. evaluate maturity of the risk management process.
C. assist in the development of a risk profile.
D. maintain a risk register based on noncompliances.

Answer: C

NEW QUESTION 820
- (Exam Topic 1)
It is MOST appropriate for changes to be promoted to production after they are:

A. communicated to business management
B. tested by business owners.
C. approved by the business owner.
D. initiated by business users.

Answer: C

NEW QUESTION 821
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CRISC Practice Exam Features:

* CRISC Questions and Answers Updated Frequently

* CRISC Practice Questions Verified by Expert Senior Certified Staff

* CRISC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

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