# Exam Questions CRISC

Certified in Risk and Information Systems Control

**https://www.2passeasy.com/dumps/CRISC/**

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

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

**Answer:** C

**NEW QUESTION 2**
- (Exam Topic 4)
When developing a response plan to address security incidents regarding sensitive data loss, it is MOST important

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

**Answer:** C

**NEW QUESTION 3**
- (Exam Topic 4)
A global company s business continuity plan (BCP) requires the transfer of its customer information…. event of a disaster. Which of the following should be the MOST important risk consideration?

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

**Answer:** B

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

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

**Answer:** D

**NEW QUESTION 5**
- (Exam Topic 4)
A highly regulated enterprise is developing a new risk management plan to specifically address legal and regulatory risk scenarios What should be done FIRST by IT governance to support this effort?

A. Request a regulatory risk reporting methodology
B. Require critical success factors (CSFs) for IT risks.
C. Establish IT-specific compliance objectives
D. Communicate IT key risk indicators (KRIs) and triggers

**Answer:** A

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

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

**Answer:** C

**NEW QUESTION 7**
- (Exam Topic 4)
A risk practitioner has collaborated with subject matter experts from the IT department to develop a large list of potential key risk indicators (KRIs) for all IT operations within the organization of the following, who should review the completed list and select the appropriate KRIs for implementation?

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

**Answer:** D

**NEW QUESTION 8**
- (Exam Topic 4)
An organization has decided to postpone the assessment and treatment of several risk scenarios because stakeholders are unavailable. As a result of this decision, the risk associated with these new entries has been;

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

**Answer:** C

**NEW QUESTION 9**
- (Exam Topic 4)
Which of the following is the BEST way to ensure data is properly sanitized while in cloud storage?

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

**Answer:** B

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

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

**Answer:** B

**NEW QUESTION 12**
- (Exam Topic 4)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

**Answer:** A

**NEW QUESTION 13**
- (Exam Topic 4)
WhichT5f the following is the MOST effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage?

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

**Answer:** B

**NEW QUESTION 15**
- (Exam Topic 4)
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, program for all employees of the organization?

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

**Answer:** C

**NEW QUESTION 20**
- (Exam Topic 4)
Using key risk indicators (KRIs) to illustrate changes in the risk profile PRIMARILY helps to:

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

**Answer:** A

**NEW QUESTION 24**
- (Exam Topic 4)
The MOST important measure of the effectiveness of risk management in project implementation is the percentage of projects:

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

**Answer:** A

**NEW QUESTION 28**
- (Exam Topic 4)
Risk appetite should be PRIMARILY driven by which of the following?

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

**Answer:** B

**NEW QUESTION 32**
- (Exam Topic 4)
Which of the following key performance indicators (KPis) would BEST measure me risk of a service outage when using a Software as a Service (SaaS) vendors

A. Frequency of business continuity plan (BCP) lasting
B. Frequency and number of new software releases
C. Frequency and duration of unplanned downtime
D. Number of IT support staff available after business hours

**Answer:** C

**NEW QUESTION 35**
- (Exam Topic 4)
Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

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

**Answer:** D

**NEW QUESTION 37**
- (Exam Topic 4)
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

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

**Answer:**

A

**NEW QUESTION 38**
- (Exam Topic 4)
Which of the following would be of MOST concern to a risk practitioner reviewing risk action plans for documented IT risk scenarios?

A. Individuals outside IT are managing action plans for the risk scenarios.
B. Target dates for completion are missing from some action plans.
C. Senior management approved multiple changes to several action plans.
D. Many action plans were discontinued after senior management accepted the risk.

**Answer:** B

**NEW QUESTION 43**
- (Exam Topic 4)
Which of the following roles should be assigned accountability for monitoring risk levels?

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

**Answer:** C

**NEW QUESTION 44**
- (Exam Topic 4)
Which of the following provides the MOST useful information for developing key risk indicators (KRIs)?

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

**Answer:** C

**NEW QUESTION 46**
- (Exam Topic 4)
Which of the following should be the FIRST consideration when establishing a new risk governance program?

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

**Answer:** B

**NEW QUESTION 48**
- (Exam Topic 4)
After undertaking a risk assessment of a production system, the MOST appropriate action is fcr the risk manager to

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

**Answer:** B

**NEW QUESTION 52**
- (Exam Topic 4)
A root because analysis indicates a major service disruption due to a lack of competency of newly hired IT system administrators Who should be accountable for resolving the situation?

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

**Answer:** C

**NEW QUESTION 55**
- (Exam Topic 4)
An organization uses one centralized single sign-on (SSO) control to cover many applications. Which of the following is the BEST course of action when a new application is added to the environment after testing of the SSO control has been completed?

A. Initiate a retest of the full control
B. Retest the control using the new application as the only sample.

C. Review the corresponding change control documentation
D. Re-evaluate the control during (he next assessment

**Answer:** A

**NEW QUESTION 57**
- (Exam Topic 4)
An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis Which of the following is the MOST important control to ensure the privacy of customer information?

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

**Answer:** C

**NEW QUESTION 62**
- (Exam Topic 4)
Which of the following is MOST important to determine when assessing the potential risk exposure of a loss event involving personal data?

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

**Answer:** C

**NEW QUESTION 64**
- (Exam Topic 4)
Which of the following is the MOST effective way to help ensure accountability for managing risk?

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

**Answer:** A

**NEW QUESTION 65**
- (Exam Topic 4)
Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

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

**Answer:** A

**NEW QUESTION 66**
- (Exam Topic 4)
Which of the following is the BEST approach for an organization in a heavily regulated industry to comprehensively test application functionality?

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

**Answer:** D

**NEW QUESTION 69**
- (Exam Topic 4)
When is the BEST to identify risk associated with major project to determine a mitigation plan?

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

**Answer:** D

**NEW QUESTION 74**
- (Exam Topic 4)
Which of the following is MOST likely to introduce risk for financial institutions that use blockchain?

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

**Answer:** B

**NEW QUESTION 77**
- (Exam Topic 4)
A recent regulatory requirement has the potential to affect an organization's use of a third party to supply outsourced business services. Which of the following is the BEST course of action?

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

**Answer:** A

**NEW QUESTION 78**
- (Exam Topic 4)
Which of The following BEST represents the desired risk posture for an organization?

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

**Answer:** D

**NEW QUESTION 82**
- (Exam Topic 4)
Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

A. Incomplete end-user device inventory
B. Unsupported end-user applications
C. Incompatible end-user devices
D. Multiple end-user device models

**Answer:** A

**NEW QUESTION 85**
- (Exam Topic 4)
A MAJOR advantage of using key risk indicators (KRis) is that (hey

A. identify when risk exceeds defined thresholds
B. assess risk scenarios that exceed defined thresholds
C. identify scenarios that exceed defined risk appetite
D. help with internal control assessments concerning risk appellate

**Answer:** B

**NEW QUESTION 88**
- (Exam Topic 4)
Which of the following is the BEST method to maintain a common view of IT risk within an organization?

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

**Answer:** C

**NEW QUESTION 91**
- (Exam Topic 4)
A multinational organization is considering implementing standard background checks to' all new employees A KEY concern regarding this approach

A. fail to identity all relevant issues.
B. be too costly
C. violate laws in other countries
D. be too line consuming

**Answer:** C

**NEW QUESTION 96**

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

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

**Answer:** C

**NEW QUESTION 97**
- (Exam Topic 3)
Which of the following BEST measures the impact of business interruptions caused by an IT service outage?

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

**Answer:** A

**NEW QUESTION 99**
- (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 103**
- (Exam Topic 3)
The PRIMARY reason for prioritizing risk scenarios is to:

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

**Answer:** D

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

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

**Answer:** A

**NEW QUESTION 110**
- (Exam Topic 4)
An organization has allowed several employees to retire early in order to avoid layoffs Many of these employees have been subject matter experts for critical assets Which type of risk is MOST likely to materialize?

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

**Answer:** B

**NEW QUESTION 111**
- (Exam Topic 4)
A legacy application used for a critical business function relies on software that has reached the end of extended support Which of the following is the MOST effective control to manage this application?

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

**Answer:** D

**NEW QUESTION 114**
- (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 115**
- (Exam Topic 3)
The BEST way to improve a risk register is to ensure the register:

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

**Answer:** A

**NEW QUESTION 118**
- (Exam Topic 3)
Which of the following is the MOST effective control to maintain the integrity of system configuration files?

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

**Answer:** D

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

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

**Answer:** D

**NEW QUESTION 122**
- (Exam Topic 3)
Which of the following is MOST useful when communicating risk to management?

A. Risk policy
B. Audit report
C. Risk map
D. Maturity model

**Answer:** C

**NEW QUESTION 126**
- (Exam Topic 3)
During a risk treatment plan review, a risk practitioner finds the approved risk action plan has not been completed However, there were other risk mitigation actions implemented. Which of the fallowing is the BEST course of action?

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

**Answer:** A

**NEW QUESTION 128**
- (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 132**
- (Exam Topic 3)
When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

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

**Answer:** D

**NEW QUESTION 134**
- (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 135**
- (Exam Topic 3)
Which of the following should be the FIRST consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected?

A. Informed consent
B. Cross border controls
C. Business impact analysis (BIA)
D. Data breach protection

**Answer:** A

**NEW QUESTION 137**
- (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 142**
- (Exam Topic 3)
The PRIMARY purpose of using a framework for risk analysis is to:

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

**Answer:** B

**NEW QUESTION 145**
- (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 149**
- (Exam Topic 3)

Which of tie following is We MOST important consideration when implementing ethical remote work monitoring?

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

**Answer:** B

**NEW QUESTION 150**
- (Exam Topic 3)
Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

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

**Answer:** A

**NEW QUESTION 153**
- (Exam Topic 3)
The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:

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

**Answer:** B

**NEW QUESTION 155**
- (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 160**
- (Exam Topic 3)
Which of the following should be an element of the risk appetite of an organization?

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

**Answer:** B

**NEW QUESTION 163**
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?

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

**Answer:** D

**NEW QUESTION 165**
- (Exam Topic 3)
Several network user accounts were recently created without the required management approvals. Which of the following would be the risk practitioner's BEST recommendation to address this situation?

A. Conduct a comprehensive compliance review.
B. Develop incident response procedures for noncompliance.
C. Investigate the root cause of noncompliance.
D. Declare a security breach and Inform management.

**Answer:** C

**NEW QUESTION 169**
- (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 174**
- (Exam Topic 3)
An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

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

**Answer:** A

**NEW QUESTION 175**
- (Exam Topic 3)
While evaluating control costs, management discovers that the annual cost exceeds the annual loss expectancy (ALE) of the risk. This indicates the:

A. control is ineffective and should be strengthened
B. risk is inefficiently controlled.
C. risk is efficiently controlled.
D. control is weak and should be removed.

**Answer:** B

**NEW QUESTION 179**
- (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 180**
- (Exam Topic 3)
Which of the following is the MOST appropriate action when a tolerance threshold is exceeded?

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

**Answer:** A

**NEW QUESTION 182**
- (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 185**
- (Exam Topic 3)
Risk acceptance of an exception to a security control would MOST likely be justified when:

A. automation cannot be applied to the control
B. business benefits exceed the loss exposure.
C. the end-user license agreement has expired.
D. the control is difficult to enforce in practice.

**Answer:**

B

**NEW QUESTION 188**
- (Exam Topic 3)
Which of the following is the PRIMARY risk management responsibility of the second line of defense?

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

**Answer:** A

**NEW QUESTION 190**
- (Exam Topic 3)
Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

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

**Answer:** C

**NEW QUESTION 194**
- (Exam Topic 3)
The MOST important reason for implementing change control procedures is to ensure:

A. only approved changes are implemented
B. timely evaluation of change events
C. an audit trail exists.
D. that emergency changes are logged.

**Answer:** A

**NEW QUESTION 198**
- (Exam Topic 3)
An organization has been notified that a disgruntled, terminated IT administrator has tried to break into the corporate network. Which of the following discoveries should be of GREATEST concern to the organization?

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

**Answer:** A

**NEW QUESTION 199**
- (Exam Topic 3)
Determining if organizational risk is tolerable requires:

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

**Answer:** D

**NEW QUESTION 200**
- (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 204**
- (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 207**
- (Exam Topic 3)
An organization discovers significant vulnerabilities in a recently purchased commercial off-the-shelf software product which will not be corrected until the next release. Which of the following is the risk manager's BEST course of action?

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

**Answer:** C

**NEW QUESTION 209**
- (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 211**
- (Exam Topic 3)
Which of the following should be of GREATEST concern lo a risk practitioner reviewing the implementation of an emerging technology?

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

**Answer:** B

**NEW QUESTION 214**
- (Exam Topic 3)
Which of the following should be the risk practitioner's FIRST course of action when an organization plans to adopt a cloud computing strategy?

A. Request a budget for implementation
B. Conduct a threat analysis.
C. Create a cloud computing policy.
D. Perform a controls assessment.

**Answer:** B

**NEW QUESTION 217**
- (Exam Topic 3)
Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

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

**Answer:** D

**NEW QUESTION 221**
- (Exam Topic 3)
A risk practitioner has been asked to advise management on developing a log collection and correlation strategy. Which of the following should be the MOST important consideration when developing this strategy?

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

**Answer:** A

**NEW QUESTION 226**

- (Exam Topic 3)
Which of the following should be included in a risk scenario to be used for risk analysis?

A. Risk appetite
B. Threat type
C. Risk tolerance
D. Residual risk

**Answer:** B

**NEW QUESTION 229**
- (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 232**
- (Exam Topic 3)
Which of the following scenarios represents a threat?

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

**Answer:** D

**NEW QUESTION 235**
- (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 238**
- (Exam Topic 3)
Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information lo a supplier?

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

**Answer:** B

**NEW QUESTION 241**
- (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 246**
- (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 247**
- (Exam Topic 3)
Which of the following criteria associated with key risk indicators (KRIs) BEST enables effective risk monitoring?

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

**Answer:** C

**NEW QUESTION 249**
- (Exam Topic 3)
The BEST way to obtain senior management support for investment in a control implementation would be to articulate the reduction in:

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

**Answer:** D

**NEW QUESTION 251**
- (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 254**
- (Exam Topic 3)
Vulnerabilities have been detected on an organization's systems. Applications installed on these systems will not operate if the underlying servers are updated. Which of the following is the risk practitioner's BEST course of action?

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

**Answer:** D

**NEW QUESTION 258**
- (Exam Topic 3)
Which of The following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?

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

**Answer:** C

**NEW QUESTION 259**
- (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 264**
- (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 265**
- (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 267**
- (Exam Topic 3)
Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?

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

**Answer:** C

**NEW QUESTION 268**
- (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 271**
- (Exam Topic 3)
Which of the following practices MOST effectively safeguards the processing of personal data?

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

**Answer:** B

**NEW QUESTION 273**
- (Exam Topic 3)
Which of the following should be management's PRIMARY consideration when approving risk response action plans?

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

**Answer:** C

**NEW QUESTION 278**
- (Exam Topic 3)
Which of the following is the GREATEST benefit for an organization with a strong risk awareness culture?

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

**Answer:** D

**NEW QUESTION 280**
- (Exam Topic 3)
Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

A. Financial risk is given a higher priority.
B. Risk with strategic impact is included.

C. Security strategy is given a higher priority.
D. Risk identified by industry benchmarking is included.

**Answer:** B

**NEW QUESTION 284**
- (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 287**
- (Exam Topic 3)
Legal and regulatory risk associated with business conducted over the Internet is driven by:

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

**Answer:** C

**NEW QUESTION 292**
- (Exam Topic 3)
Winch of the following is the BEST evidence of an effective risk treatment plan?

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

**Answer:** B

**NEW QUESTION 296**
- (Exam Topic 3)
Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?

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

**Answer:** D

**NEW QUESTION 298**
- (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 300**
- (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 305**
- (Exam Topic 3)
Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures?

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

**Answer:** D

**NEW QUESTION 307**
- (Exam Topic 3)
Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

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

**Answer:** D

**NEW QUESTION 308**
- (Exam Topic 3)
What are the MOST essential attributes of an effective Key control indicator (KCI)?

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

**Answer:** B

**NEW QUESTION 309**
- (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 312**
- (Exam Topic 3)
Which of the following is the MOST important component in a risk treatment plan?

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

**Answer:** D

**NEW QUESTION 317**
- (Exam Topic 3)
The PRIMARY objective of a risk identification process is to:

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

**Answer:** B

**NEW QUESTION 319**
- (Exam Topic 3)
What is the PRIMARY benefit of risk monitoring?

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

**Answer:** C

**NEW QUESTION 323**
- (Exam Topic 3)

When updating the risk register after a risk assessment, which of the following is MOST important to include?

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

**Answer:** C

**NEW QUESTION 327**
- (Exam Topic 3)
A risk practitioner is developing a set of bottom-up IT risk scenarios. The MOST important time to involve business stakeholders is when:

A. updating the risk register
B. documenting the risk scenarios.
C. validating the risk scenarios
D. identifying risk mitigation controls.

**Answer:** C

**NEW QUESTION 329**
- (Exam Topic 3)
When reporting on the performance of an organization's control environment including which of the following would BEST inform stakeholders risk decision-making?

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

**Answer:** C

**NEW QUESTION 330**
- (Exam Topic 3)
Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

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

**Answer:** C

**NEW QUESTION 334**
- (Exam Topic 3)
What should be the PRIMARY driver for periodically reviewing and adjusting key risk indicators (KRIs)?

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

**Answer:** B

**NEW QUESTION 338**
- (Exam Topic 3)
Who should be accountable for monitoring the control environment to ensure controls are effective?

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

**Answer:** A

**NEW QUESTION 343**
- (Exam Topic 3)
Which of the following BEST facilities the alignment of IT risk management with enterprise risk management (ERM)?

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

**Answer:** C

**NEW QUESTION 348**
- (Exam Topic 3)
Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

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

**Answer:** A

**NEW QUESTION 350**
- (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 353**
- (Exam Topic 3)
Which of the following risk management practices BEST facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register?

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

**Answer:** D

**NEW QUESTION 355**
- (Exam Topic 3)
The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

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

**Answer:** D

**NEW QUESTION 357**
- (Exam Topic 3)
Which of the following would BEST indicate to senior management that IT processes are improving?

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

**Answer:** B

**NEW QUESTION 362**
- (Exam Topic 3)
Which of the following controls BEST enables an organization to ensure a complete and accurate IT asset inventory?

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

**Answer:** B

**NEW QUESTION 366**
- (Exam Topic 3)
Which of the following should be a risk practitioner's PRIMARY focus when tasked with ensuring organization records are being retained for a sufficient period of time to meet legal obligations?

A. Data duplication processes
B. Data archival processes
C. Data anonymization processes
D. Data protection processes

**Answer:**

B

**NEW QUESTION 370**
- (Exam Topic 3)
Which of the following methods is an example of risk mitigation?

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

**Answer:** C

**NEW QUESTION 374**
- (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 376**
- (Exam Topic 3)
In which of the following system development life cycle (SDLC) phases should controls be incorporated into system specifications?

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

**Answer:** C

**NEW QUESTION 380**
- (Exam Topic 3)
Which of the following is the BEST way to quantify the likelihood of risk materialization?

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

**Answer:** D

**NEW QUESTION 383**
- (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 385**
- (Exam Topic 3)
Which of the following would be MOST helpful when communicating roles associated with the IT risk management process?

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

**Answer:** A

**NEW QUESTION 390**
- (Exam Topic 3)
Who is BEST suited to determine whether a new control properly mitigates data loss risk within a system?

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

**Answer:** B

**NEW QUESTION 392**
- (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 396**
- (Exam Topic 3)
Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

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

**Answer:** B

**NEW QUESTION 400**
- (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 404**
- (Exam Topic 3)
Which of the following controls BEST helps to ensure that transaction data reaches its destination?

A. Securing the network from attacks
B. Providing acknowledgments from receiver to sender
C. Digitally signing individual messages
D. Encrypting data-in-transit

**Answer:** B

**NEW QUESTION 409**
- (Exam Topic 3)
All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

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

**Answer:** D

**NEW QUESTION 410**
- (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 413**
- (Exam Topic 4)
The objective of aligning mitigating controls to risk appetite is to ensure that:

A. exposures are reduced to the fullest extent

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

**Answer:** D

**NEW QUESTION 414**
- (Exam Topic 4)
Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

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

**Answer:** A

**NEW QUESTION 417**
- (Exam Topic 4)
Which of the following situations presents the GREATEST challenge to creating a comprehensive IT risk profile of an organization?

A. Manual vulnerability scanning processes
B. Organizational reliance on third-party service providers
C. Inaccurate documentation of enterprise architecture (EA)
D. Risk-averse organizational risk appetite

**Answer:** D

**NEW QUESTION 420**
- (Exam Topic 4)
Which of the following is MOST important to ensure when reviewing an organization's risk register?

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

**Answer:** A

**NEW QUESTION 421**
- (Exam Topic 4)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

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

**Answer:** C

**NEW QUESTION 425**
- (Exam Topic 4)
Which of the following is the MOST important characteristic of a key risk indicator (KRI) to enable decision-making?

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

**Answer:** D

**NEW QUESTION 427**
- (Exam Topic 4)
Recovery the objectives (RTOs) should be based on

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

**Answer:** C

**NEW QUESTION 429**
- (Exam Topic 4)
Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud

environment?

A. Reviewing the results of independent audits
B. Performing a site visit to the cloud provider's data center
C. Performing a due diligence review
D. Conducting a risk workshop with key stakeholders

**Answer:** D

**NEW QUESTION 431**
- (Exam Topic 4)
An organization has an approved bring your own device (BYOD) policy. Which of the following would BEST mitigate the security risk associated with the inappropriate use of enterprise applications on the devices?

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

**Answer:** C

**NEW QUESTION 435**
- (Exam Topic 4)
A company has recently acquired a customer relationship management (CRM) application from a certified software vendor. Which of the following will BE ST help lo prevent technical vulnerabilities from being exploded?

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

**Answer:** D

**NEW QUESTION 436**
- (Exam Topic 4)
A risk practitioner recently discovered that personal information from the production environment is required for testing purposes in non-production environments. Which of the following is the BEST recommendation to address this situation?

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

**Answer:** C

**NEW QUESTION 440**
- (Exam Topic 4)
Reviewing which of the following BEST helps an organization gam insight into its overall risk profile"

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

**Answer:** B

**NEW QUESTION 444**
- (Exam Topic 4)
Which of the following is the BEST way to ensure adequate resources will be allocated to manage identified risk?

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

**Answer:** D

**NEW QUESTION 449**
- (Exam Topic 4)
Which of the following will BEST help to ensure the continued effectiveness of the IT risk management function within an organization experiencing high employee turnover?

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

**Answer:** B

**NEW QUESTION 451**
- (Exam Topic 4)
An organization has agreed to a 99% availability for its online services and will not accept availability that falls below 98.5%. This is an example of:

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

**Answer:** C

**NEW QUESTION 456**
- (Exam Topic 4)
Which risk response strategy could management apply to both positive and negative risk that has been identified?

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

**Answer:** B

**NEW QUESTION 457**
- (Exam Topic 4)
Which of the following BEST enables senior management lo compare the ratings of risk scenarios?

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

**Answer:** D

**NEW QUESTION 460**
- (Exam Topic 4)
Who should be responsible (of evaluating the residual risk after a compensating control has been

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

**Answer:** D

**NEW QUESTION 461**
- (Exam Topic 4)
An organization is analyzing the risk of shadow IT usage. Which of the following is the MOST important input into the assessment?

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

**Answer:** A

**NEW QUESTION 466**
- (Exam Topic 4)
Which of the following would BEST facilitate the implementation of data classification requirements?

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

**Answer:** B

**NEW QUESTION 469**
- (Exam Topic 4)
Which of the following has the GREATEST influence on an organization's risk appetite?

A. Threats and vulnerabilities
B. Internal and external risk factors
C. Business objectives and strategies

D. Management culture and behavior

**Answer:** D

**NEW QUESTION 471**
- (Exam Topic 4)
Which of the following will BEST help to ensure new IT policies address the enterprise's requirements?

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

**Answer:** B

**NEW QUESTION 473**
- (Exam Topic 4)
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

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

**Answer:** D

**NEW QUESTION 476**
- (Exam Topic 4)
Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

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

**Answer:** B

**NEW QUESTION 480**
- (Exam Topic 4)
When of the following standard operating procedure (SOP) statements BEST illustrates appropriate risk register maintenance?

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

**Answer:** C

**NEW QUESTION 482**
- (Exam Topic 4)
When performing a risk assessment of a new service to support a core business process, which of the following should be done FIRST to ensure continuity of operations?

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

**Answer:** B

**NEW QUESTION 484**
- (Exam Topic 4)
What is the PRIMARY reason an organization should include background checks on roles with elevated access to production as part of its hiring process?

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

**Answer:** C

**NEW QUESTION 489**
- (Exam Topic 4)
Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

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

**Answer:** A

**NEW QUESTION 494**
- (Exam Topic 4)
Which of the following BEST enables effective IT control implementation?

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

**Answer:** B

**NEW QUESTION 498**
- (Exam Topic 4)
Which of the following contributes MOST to the effective implementation of risk responses?

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

**Answer:** A

**NEW QUESTION 502**
- (Exam Topic 4)
Which of the following is the MOST important course of action for a risk practitioner when reviewing the results of control performance monitoring?

A. Evaluate changes to the organization's risk profile.
B. Validate whether the controls effectively mitigate risk.
C. Confirm controls achieve regulatory compliance.
D. Analyze appropriateness of key performance indicators (KPIs).

**Answer:** D

**NEW QUESTION 506**
- (Exam Topic 4)
A zero-day vulnerability has been discovered in a globally used brand of hardware server that allows hackers to gain access to affected IT systems. Which of the following is MOST likely to change as a result of this situation?

A. Control effectiveness
B. Risk appetite
C. Risk likelihood
D. Key risk indicator (KRI)

**Answer:** C

**NEW QUESTION 511**
- (Exam Topic 4)
The BEST indicator of the risk appetite of an organization is the

A. regulatory environment of the organization
B. risk management capability of the organization
C. board of directors' response to identified risk factors
D. importance assigned to IT in meeting strategic goals

**Answer:** B

**NEW QUESTION 516**
- (Exam Topic 4)
A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner s NEXT step? r

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

**Answer:** D

**NEW QUESTION 520**

- (Exam Topic 4)
The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

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

**Answer:** C

**NEW QUESTION 523**
- (Exam Topic 4)
An organization has operations in a location that regularly experiences severe weather events. Which of the following would BEST help to mitigate the risk to operations?

A. Prepare a cost-benefit analysis to evaluate relocation.
B. Prepare a disaster recovery plan (DRP).
C. Conduct a business impact analysis (BIA) for an alternate location.
D. Develop a business continuity plan (BCP).

**Answer:** D

**NEW QUESTION 527**
- (Exam Topic 4)
One of an organization's key IT systems cannot be patched because the patches interfere with critical business application functionalities. Which of the following would be the risk practitioner's BEST recommendation?

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

**Answer:** A

**NEW QUESTION 531**
- (Exam Topic 4)
Which of the following is the PRIMARY reason for an organization to include an acceptable use banner when users log in?

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

**Answer:** A

**NEW QUESTION 533**
- (Exam Topic 4)
Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

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

**Answer:** A

**NEW QUESTION 537**
- (Exam Topic 4)
A global organization has implemented an application that does not address all privacy requirements across multiple jurisdictions. Which of the following risk responses has the organization adopted with regard to privacy requirements?

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

**Answer:** A

**NEW QUESTION 540**
- (Exam Topic 4)
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 541**
- (Exam Topic 4)
An organization wants to launch a campaign to advertise a new product Using data analytics, the campaign can be targeted to reach potential customers. Which of the following should be of GREATEST concern to the risk practitioner?

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

**Answer:** D

**NEW QUESTION 542**
- (Exam Topic 4)
When documenting a risk response, which of the following provides the STRONGEST evidence to support the decision?

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

**Answer:** C

**NEW QUESTION 547**
- (Exam Topic 4)
An organization recently configured a new business division Which of the following is MOST likely to be affected?

A. Risk profile
B. Risk culture
C. Risk appetite
D. Risk tolerance

**Answer:** A

**NEW QUESTION 551**
- (Exam Topic 4)
Which of the following is the BEST recommendation to address recent IT risk trends that indicate social engineering attempts are increasing in the organization?

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

**Answer:** A

**NEW QUESTION 555**
- (Exam Topic 4)
Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

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

**Answer:** C

**NEW QUESTION 558**
- (Exam Topic 4)
Which of the following s MOST likely to deter an employee from engaging in inappropriate use of company owned IT systems?

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

**Answer:** D

**NEW QUESTION 559**
- (Exam Topic 4)
Who is MOST appropriate to be assigned ownership of a control

A. The individual responsible for control operation

B. The individual informed of the control effectiveness
C. The individual responsible for resting the control
D. The individual accountable for monitoring control effectiveness

**Answer:** D

**NEW QUESTION 563**
- (Exam Topic 4)
Which of the following is the BEST method to mitigate the risk of an unauthorized employee viewing confidential data in a database"

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

**Answer:** A

**NEW QUESTION 566**
- (Exam Topic 4)
Which of the following is MOST helpful in identifying loss magnitude during risk analysis of a new system?

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

**Answer:** C

**NEW QUESTION 569**
- (Exam Topic 4)
An organization's recovery team is attempting to recover critical data backups following a major flood in its data center. However, key team members do not know exactly what steps should be taken to address this crisis. Which of the following is the MOST likely cause of this situation?

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

**Answer:** A

**NEW QUESTION 570**
- (Exam Topic 4)
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

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

**Answer:** A

**NEW QUESTION 575**
- (Exam Topic 4)
An organization plans to implement a new Software as a Service (SaaS) speech-to-text solution Which of the following is MOST important to mitigate risk associated with data privacy?

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

**Answer:** A

**NEW QUESTION 577**
- (Exam Topic 4)
Which of the following is MOST important for successful incident response?

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

**Answer:** D

**NEW QUESTION 578**

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

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

**Answer:** A

**NEW QUESTION 582**
- (Exam Topic 4)
Which of the following is the PRIMARY objective of maintaining an information asset inventory?

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

**Answer:** B

**NEW QUESTION 587**
- (Exam Topic 4)
Which of the following is MOST helpful in providing an overview of an organization's risk management program?

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

**Answer:** C

**NEW QUESTION 590**
- (Exam Topic 4)
Which of the following is the PRIMARY reason to perform periodic vendor risk assessments?

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

**Answer:** B

**NEW QUESTION 594**
- (Exam Topic 4)
Which of the following BEST reduces the risk associated with the theft of a laptop containing sensitive information?

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

**Answer:** B

**NEW QUESTION 595**
- (Exam Topic 4)
Which of the following is the BEST method of creating risk awareness in an organization?

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

**Answer:** B

**NEW QUESTION 597**
- (Exam Topic 4)
Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

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

**Answer:** A

**NEW QUESTION 599**
- (Exam Topic 4)
Which of the following is the BEST way to protect sensitive data from administrators within a public cloud?

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

**Answer:** D

**NEW QUESTION 603**
- (Exam Topic 4)
Which of the following is the BEST course of action when an organization wants to reduce likelihood in order to reduce a risk level?

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

**Answer:** B

**NEW QUESTION 605**
- (Exam Topic 4)
Effective risk communication BEST benefits an organization by:

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

**Answer:** A

**NEW QUESTION 610**
- (Exam Topic 4)
Which of the following is a risk practitioner's BEST recommendation upon learning that an employee inadvertently disclosed sensitive data to a vendor?

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

**Answer:** B

**NEW QUESTION 615**
- (Exam Topic 4)
Which of the following is MOST useful for measuring the existing risk management process against a desired state?

A. Balanced scorecard
B. Risk management framework
C. Capability maturity model
D. Risk scenario analysis

**Answer:** C

**NEW QUESTION 618**
- (Exam Topic 4)
Which of the following is MOST important for senior management to review during an acquisition?

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

**Answer:** A

**NEW QUESTION 621**
- (Exam Topic 4)
Which key performance efficiency IKPI) BEST measures the effectiveness of an organization's disaster recovery program?

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

**Answer:** D

**NEW QUESTION 626**
- (Exam Topic 4)
After an annual risk assessment is completed, which of the following would be MOST important to communicate to stakeholders?

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

**Answer:** B

**NEW QUESTION 631**
- (Exam Topic 4)
Which of the following would be the GREATEST concern for an IT risk practitioner when an employees.....

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

**Answer:** B

**NEW QUESTION 634**
- (Exam Topic 4)
A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which ot the following is the risk practitioner's BEST course of action?

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

**Answer:** A

**NEW QUESTION 639**
- (Exam Topic 4)
What is the BEST recommendation to reduce the risk associated with potential system compromise when a vendor stops releasing security patches and updates for a business-critical legacy system?

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

**Answer:** A

**NEW QUESTION 644**
- (Exam Topic 4)
Who is the BEST person to the employee personal data?

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

**Answer:** A

**NEW QUESTION 648**
- (Exam Topic 4)
Of the following, who is responsible for approval when a change in an application system is ready for release to production?

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

**Answer:** C

**NEW QUESTION 651**
- (Exam Topic 4)
It is MOST important that security controls for a new system be documented in:

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

**Answer:** C

**NEW QUESTION 653**
- (Exam Topic 4)
Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

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

**Answer:** A

**NEW QUESTION 655**
- (Exam Topic 4)
When evaluating a number of potential controls for treating risk, it is MOST important to consider:

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

**Answer:** C

**NEW QUESTION 656**
- (Exam Topic 4)
Which of the following is the GREATEST concern when establishing key risk indicators (KRIs)?

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

**Answer:** B

**NEW QUESTION 657**
- (Exam Topic 4)
Which organization is implementing a project to automate the purchasing process, including the modification of approval controls. Which of the following tasks is lie responsibility of the risk practitioner*?

A. Verify that existing controls continue to properly mitigate defined risk
B. Test approval process controls once the project is completed
C. Update the existing controls for changes in approval processes from this project
D. Perform a gap analysis of the impacted control processes

**Answer:** B

**NEW QUESTION 662**
- (Exam Topic 4)
Which of the following is MOST important to determine as a result of a risk assessment?

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

**Answer:** D

**NEW QUESTION 666**
- (Exam Topic 4)
Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

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

**Answer:** A

**NEW QUESTION 667**
- (Exam Topic 4)
A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

A. Risk manager

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

**Answer:** B

**NEW QUESTION 668**
- (Exam Topic 4)
Which of the following should be the PRIMARY input to determine risk tolerance?

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

**Answer:** C

**NEW QUESTION 669**
- (Exam Topic 4)
A bank recently incorporated Blockchain technology with the potential to impact known risk within the organization. Which of the following is the risk practitioner's BEST course of action?

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

**Answer:** B

**NEW QUESTION 670**
- (Exam Topic 4)
After entering a large number of low-risk scenarios into the risk register, it is MOST important for the risk practitioner to:

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

**Answer:** D

**NEW QUESTION 671**
- (Exam Topic 4)
Which of the following should be the PRIMARY basis for prioritizing risk responses?

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

**Answer:** A

**NEW QUESTION 674**
- (Exam Topic 4)
Which of the following is MOST important when determining risk appetite?

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

**Answer:** C

**NEW QUESTION 679**
- (Exam Topic 4)
Which of the following would MOST effectively reduce risk associated with an increase of online transactions on a retailer website?

A. Scalable infrastructure
B. A hot backup site
C. Transaction limits
D. Website activity monitoring

**Answer:** C

**NEW QUESTION 680**
- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 683**
- (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 688**
- (Exam Topic 3)
Which of the following would MOST likely cause a risk practitioner to change the likelihood rating in the risk register?

A. Risk appetite
B. Control cost
C. Control effectiveness
D. Risk tolerance

**Answer:** C

**NEW QUESTION 690**
- (Exam Topic 3)
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual
risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

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

**Answer:** D

**NEW QUESTION 691**
- (Exam Topic 3)
To minimize the risk of a potential acquisition being exposed externally, an organization has selected a few
key employees to be engaged in the due diligence process. A member of the due diligence team realizes a close acquaintance is a high-ranking IT professional at a subsidiary of the company about to be acquired. What is the BEST course of action for this team member?

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

**Answer:** B

**NEW QUESTION 695**
- (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 699**
- (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 704**
- (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 709**
- (Exam Topic 3)
Which of the following describes the relationship between Key risk indicators (KRIs) and key control indicators (KCIS)?

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

**Answer:** D

**NEW QUESTION 713**
- (Exam Topic 3)
An information system for a key business operation is being moved from an in-house application to a Software as a Service (SaaS) vendor. Which of the following will have the GREATEST impact on the ability to monitor risk?

A. Reduced ability to evaluate key risk indicators (KRIs)
B. Reduced access to internal audit reports
C. Dependency on the vendor's key performance indicators (KPIs)
D. Dependency on service level agreements (SLAs)

**Answer:** A

**NEW QUESTION 718**
- (Exam Topic 3)
When an organization’s disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?

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

**Answer:** B

**NEW QUESTION 719**
- (Exam Topic 3)
A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

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

**Answer:** D

**NEW QUESTION 720**
- (Exam Topic 3)
When developing a risk awareness training program, which of the following training topics would BEST facilitate a thorough understanding of risk scenarios?

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

**Answer:** D

**NEW QUESTION 724**
- (Exam Topic 3)
What is the PRIMARY purpose of a business impact analysis (BIA)?

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

**Answer:** D

**NEW QUESTION 727**
- (Exam Topic 3)
A risk practitioner has been asked by executives to explain how existing risk treatment plans would affect risk posture at the end of the year. Which of the following is MOST helpful in responding to this request?

A. Assessing risk with no controls in place
B. Showing projected residual risk
C. Providing peer benchmarking results
D. Assessing risk with current controls in place

**Answer:** D

**NEW QUESTION 731**
- (Exam Topic 3)
Which of the following BEST informs decision-makers about the value of a notice and consent control for the collection of personal information?

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

**Answer:** D

**NEW QUESTION 735**
- (Exam Topic 3)
An organization planning to transfer and store its customer data with an offshore cloud service provider should be PRIMARILY concerned with:

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

**Answer:** B

**NEW QUESTION 738**
- (Exam Topic 3)
Which of the following would be the GREATEST challenge when implementing a corporate risk framework for a global organization?

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

**Answer:** A

**NEW QUESTION 741**
- (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 745**

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

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

**Answer:** A

**NEW QUESTION 746**
- (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 747**
- (Exam Topic 3)
Senior management has asked a risk practitioner to develop technical risk scenarios related to a recently developed enterprise resource planning (ERP) system. These scenarios will be owned by the system manager. Which of the following would be the BEST method to use when developing the scenarios?

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

**Answer:** A

**NEW QUESTION 748**
- (Exam Topic 3)
A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

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

**Answer:** A

**NEW QUESTION 750**
- (Exam Topic 3)
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

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

**Answer:** A

**NEW QUESTION 752**
- (Exam Topic 3)
Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

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

**Answer:** C

**NEW QUESTION 757**
- (Exam Topic 3)
Which of the following should be done FIRST when developing a data protection management plan?

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

**Answer:** B

**NEW QUESTION 759**
- (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 760**
- (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 761**
- (Exam Topic 3)
Which of the following poses the GREATEST risk to an organization's operations during a major it transformation?

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

**Answer:** D

**NEW QUESTION 762**
- (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 767**
- (Exam Topic 3)
Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

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

**Answer:** B

**NEW QUESTION 769**
- (Exam Topic 3)
The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

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

**Answer:** A

**NEW QUESTION 771**
- (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 772**
- (Exam Topic 3)
The MAIN purpose of reviewing a control after implementation is to validate that the control:

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

**Answer:** A

**NEW QUESTION 774**
- (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 777**
- (Exam Topic 3)
Which of the following BEST indicates the efficiency of a process for granting access privileges?

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

**Answer:** C

**NEW QUESTION 779**
- (Exam Topic 3)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery test of critical business processes?

A. Percentage of job failures identified and resolved during the recovery process
B. Percentage of processes recovered within the recovery time and point objectives
C. Number of current test plans and procedures
D. Number of issues and action items resolved during the recovery test

**Answer:** B

**NEW QUESTION 783**
- (Exam Topic 3)
A maturity model is MOST useful to an organization when it:

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

**Answer:** C

**NEW QUESTION 788**
- (Exam Topic 3)
A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

A. Obtain the risk owner's approval.
B. Record the risk as accepted in the risk register.
C. Inform senior management.
D. update the risk response plan.

**Answer:** A

**NEW QUESTION 791**
- (Exam Topic 3)
Which of the following is the BEST way for an organization to enable risk treatment decisions?

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

**Answer:** C

**NEW QUESTION 794**
- (Exam Topic 3)
Which of the following should be done FIRST when information is no longer required to support business objectives?

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

**Answer:** C

**NEW QUESTION 798**
- (Exam Topic 3)
Which of the following is the MOST common concern associated with outsourcing to a service provider?

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

**Answer:** C

**NEW QUESTION 801**
- (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 804**
- (Exam Topic 3)
To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:

A. require the vendor to sign a nondisclosure agreement
B. clearly define the project scope.
C. perform background checks on the vendor.
D. notify network administrators before testing

**Answer:** A

**NEW QUESTION 808**
- (Exam Topic 3)
Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

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

**Answer:** C

**NEW QUESTION 809**
- (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 810**
- (Exam Topic 3)
For a large software development project, risk assessments are MOST effective when performed:

A. before system development begins.
B. at system development.

C. at each stage of the system development life cycle (SDLC).
D. during the development of the business case.

**Answer:** C

**NEW QUESTION 814**
- (Exam Topic 3)
Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?

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

**Answer:** B

**NEW QUESTION 819**
- (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 823**
- (Exam Topic 3)
When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction based on:

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

**Answer:** A

**NEW QUESTION 827**
- (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 828**
- (Exam Topic 3)
Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:

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

**Answer:** B

**NEW QUESTION 830**
- (Exam Topic 3)
Which of the following is the FIRST step when conducting a business impact analysis (BIA)?

A. Identifying critical information assets
B. Identifying events impacting continuity of operations;
C. Creating a data classification scheme
D. Analyzing previous risk assessment results

**Answer:** A

**NEW QUESTION 834**
- (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 835**
- (Exam Topic 3)
Which of the following should be the MOST important consideration when performing a vendor risk assessment?

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

**Answer:** B

**NEW QUESTION 839**
- (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 841**
- (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 845**
- (Exam Topic 3)
Which of the following is the MOST effective way to integrate risk and compliance management?

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

**Answer:** A

**NEW QUESTION 850**
- (Exam Topic 3)
Which of the following would BEST help to address the risk associated with malicious outsiders modifying application data?

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

**Answer:** A

**NEW QUESTION 855**
- (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 860**
- (Exam Topic 3)
Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?

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

**Answer:** D

**NEW QUESTION 863**
- (Exam Topic 2)
An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

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

**Answer:** A

**NEW QUESTION 868**
- (Exam Topic 2)
Which of the following is MOST important for an organization that wants to reduce IT operational risk?

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

**Answer:** C

**NEW QUESTION 873**
- (Exam Topic 2)
Which of the following risk scenarios would be the GREATEST concern as a result of a single sign-on implementation?

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

**Answer:** B

**NEW QUESTION 876**
- (Exam Topic 2)
A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner's FIRST course of action?

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

**Answer:** D

**NEW QUESTION 880**
- (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 882**
- (Exam Topic 2)
The purpose of requiring source code escrow in a contractual agreement is to:

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

**Answer:**

B

**NEW QUESTION 887**
- (Exam Topic 2)
Which of the following is MOST helpful in developing key risk indicator (KRI) thresholds?

A. Loss expectancy information
B. Control performance predictions
C. IT service level agreements (SLAs)
D. Remediation activity progress

**Answer:** A

**NEW QUESTION 888**
- (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 889**
- (Exam Topic 2)
A risk practitioner notices that a particular key risk indicator (KRI) has remained below its established trigger point for an extended period of time. Which of the following should be done FIRST?

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

**Answer:** A

**NEW QUESTION 890**
- (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 892**
- (Exam Topic 2)
An organization's risk practitioner learns a new third-party system on the corporate network has introduced vulnerabilities that could compromise corporate IT systems. What should the risk practitioner do
FIRST?

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

**Answer:** B

**NEW QUESTION 895**
.....

# THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CRISC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CRISC Product From:

**https://www.2passeasy.com/dumps/CRISC/**

## Money Back Guarantee

## 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