

Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control



NEW QUESTION 1

- (Exam Topic 4)

When developing a response plan to address security incidents regarding sensitive data loss, it is MOST important

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

Answer: C

NEW QUESTION 2

- (Exam Topic 4)

A global company's business continuity plan (BCP) requires the transfer of its customer information.... event of a disaster. Which of the following should be the MOST important risk consideration?

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

Answer: B

NEW QUESTION 3

- (Exam Topic 4)

A 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 4

- (Exam Topic 4)

Which of the following is the MOST important consideration for effectively maintaining a risk register?

- A. An IT owner is assigned for each risk scenario.
- B. The register is updated frequently.
- C. The register is shared with executive management.
- D. Compensating controls are identified.

Answer: B

NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (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 9

- (Exam Topic 4)

Which of the following is the GREATEST benefit of having a mature enterprise architecture (EA) in place?

- A. Standards-based policies
- B. Audit readiness
- C. Efficient operations
- D. Regulatory compliance

Answer: C

NEW QUESTION 10

- (Exam Topic 4)

Which of 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-wide phishing simulations.
- C. Require training on the data handling policy.
- D. Require regular testing of the data breach response plan.

Answer: B

NEW QUESTION 10

- (Exam Topic 4)

Which of the following would provide the MOST reliable evidence of the effectiveness of security controls implemented for a web application?

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

Answer: A

NEW QUESTION 13

- (Exam Topic 4)

The BEST metric to demonstrate that servers are configured securely is the total number of servers:

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

Answer: D

NEW QUESTION 15

- (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 17

- (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 21

- (Exam Topic 4)

Which of the following key performance indicators (KPIs) would BEST measure the risk of a service outage when using a Software as a Service (SaaS) vendors

- A. Frequency of business continuity plan (BCP) testing
- 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 25

- (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 26

- (Exam Topic 4)

An organization is considering outsourcing user administration controls for a critical system. The potential vendor has offered to perform quarterly self-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to the risk practitioner?

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

Answer: D

NEW QUESTION 31

- (Exam Topic 4)

A risk practitioner notices a risk scenario associated with data loss at the organization's cloud provider is assigned to the provider. Who should the risk scenario be reassigned to?

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

Answer: D

NEW QUESTION 33

- (Exam Topic 4)

Which of the following is the GREATEST benefit of using IT risk scenarios?

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

Answer: C

NEW QUESTION 34

- (Exam Topic 4)

Which component of a software inventory BEST enables the identification and mitigation of known vulnerabilities?

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

Answer: A

NEW QUESTION 36

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 39

- (Exam Topic 4)

Which of the following, who should be PRIMARILY responsible for performing user entitlement reviews?

- A. IT security manager
- B. IT personnel
- C. Data custodian
- D. Data owner

Answer: D

NEW QUESTION 40

- (Exam Topic 4)

Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

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

Answer: D

NEW QUESTION 43

- (Exam Topic 4)

After undertaking a risk assessment of a production system, the MOST appropriate action is for 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 44

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 45

- (Exam Topic 4)

An organization has decided to commit to a business activity with the knowledge that the risk exposure is higher than the risk appetite. Which of the following is the risk practitioner's MOST important action related to this decision?

- A. Recommend risk remediation
- B. Change the level of risk appetite
- C. Document formal acceptance of the risk
- D. Reject the business initiative

Answer: C

NEW QUESTION 48

- (Exam Topic 4)

When establishing an enterprise IT risk management program, it is MOST important to:

- A. review alignment with the organizations strategy.
- B. understand the organization's information security policy.
- C. validate the organization's data classification scheme.
- D. report identified IT risk scenarios to senior management.

Answer: D

NEW QUESTION 52

- (Exam Topic 4)

Which of the following is the PRIMARY reason for a risk practitioner to review an organization's IT asset inventory?

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

Answer: C

NEW QUESTION 54

- (Exam Topic 4)

Which of the following would be a risk practitioner's GREATEST concern with the use of a vulnerability scanning tool?

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

Answer: B

NEW QUESTION 56

- (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 60

- (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 64

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 65

- (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 66

- (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 67

- (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 69

- (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 71

- (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 72

- (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 77

- (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 78

- (Exam Topic 3)

A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 82

- (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 84

- (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 88

- (Exam Topic 4)

A risk practitioner implemented a process to notify management of emergency changes that may not be approved. Which of the following is the BEST way to provide this information to management?

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

Answer: C

NEW QUESTION 93

- (Exam Topic 4)

Which of the following would MOST likely cause management to unknowingly accept excessive risk?

- A. Satisfactory audit results
- B. Risk tolerance being set too low
- C. Inaccurate risk ratings
- D. Lack of preventive controls

Answer: C

NEW QUESTION 96

- (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 97

- (Exam Topic 4)

Which of the following BEST enables risk-based decision making in support of a business continuity plan (BCP)?

- A. Impact analysis
- B. Control analysis
- C. Root cause analysis
- D. Threat analysis

Answer: A

NEW QUESTION 100

- (Exam Topic 4)

Which of the following resources is MOST helpful to a risk practitioner when updating the likelihood rating in the risk register?

- A. Risk control assessment
- B. Audit reports with risk ratings
- C. Penetration test results
- D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 105

- (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 110

- (Exam Topic 3)

Which of the following is the BEST way to determine the potential organizational impact of emerging privacy regulations?

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

Answer: D

NEW QUESTION 113

- (Exam Topic 3)

An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course of action?

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

Answer: B

NEW QUESTION 116

- (Exam Topic 3)

A violation of segregation of duties is when the same:

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

Answer: D

NEW QUESTION 121

- (Exam Topic 3)

An organization has initiated a project to launch an IT-based service to customers and take advantage of being the first to market. Which of the following should be of GREATEST concern to senior management?

- A. More time has been allotted for testing.
- B. The project is likely to deliver the product late.
- C. A new project manager is handling the project.
- D. The cost of the project will exceed the allotted budget.

Answer: B

NEW QUESTION 122

- (Exam Topic 3)

Which of the following is MOST helpful in preventing risk events from materializing?

- A. Prioritizing and tracking issues
- B. Establishing key risk indicators (KRIs)
- C. Reviewing and analyzing security incidents
- D. Maintaining the risk register

Answer: A

NEW QUESTION 123

- (Exam Topic 3)

The PRIMARY benefit associated with key risk indicators (KRIs) is that they:

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

Answer: D

NEW QUESTION 126

- (Exam Topic 3)

Which of the following will help ensure the elective decision-making of an IT risk management committee?

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

Answer: D

NEW QUESTION 130

- (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 132

- (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 134

- (Exam Topic 3)

Which of the following is the MOST appropriate key risk indicator (KRI) for backup media that is recycled monthly?

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

Answer: D

NEW QUESTION 139

- (Exam Topic 3)

Which of the following would require updates to an organization's IT risk register?

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

Answer: A

NEW QUESTION 144

- (Exam Topic 3)

Which of the following is the 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 being 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 149

- (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 151

- (Exam Topic 3)

Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

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

Answer: D

NEW QUESTION 155

- (Exam Topic 3)

From a risk management perspective, the PRIMARY objective of using maturity models is to enable:

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

Answer: C

NEW QUESTION 160

- (Exam Topic 3)

Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

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

Answer: B

NEW QUESTION 162

- (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 163

- (Exam Topic 3)

An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?

- A. Risk manager
- B. Data owner
- C. End user
- D. IT department

Answer: D

NEW QUESTION 165

- (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 167

- (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 172

- (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 176

- (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 179

- (Exam Topic 3)

Which of the following represents a vulnerability?

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

Answer: C

NEW QUESTION 183

- (Exam Topic 3)

Which of the following is MOST important for an organization to update following a change in legislation requiring notification to individuals impacted by data breaches?

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

Answer: C

NEW QUESTION 188

- (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 189

- (Exam Topic 3)

When performing a risk assessment of a new service to support a new Business process, which of the following should be done FIRST to ensure continuity of operations?

- A. identify 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 192

- (Exam Topic 3)

Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?

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

Answer: B

NEW QUESTION 196

- (Exam Topic 3)

While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BEST reduce the risk associated with such a data breach?

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

Answer: B

NEW QUESTION 197

- (Exam Topic 3)

Which of the following is the BEST evidence that a user account has been properly authorized?

- A. An email from the user accepting the account
- B. Notification from human resources that the account is active
- C. User privileges matching the request form
- D. Formal approval of the account by the user's manager

Answer: C

NEW QUESTION 198

- (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 199

- (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 202

- (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 206

- (Exam Topic 3)

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

- A. The number of users who can access sensitive data
- B. A list of unencrypted databases which contain sensitive data

- C. The reason some databases have not been encrypted
- D. The cost required to enforce encryption

Answer: B

NEW QUESTION 209

- (Exam Topic 3)

An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?

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

Answer: B

NEW QUESTION 214

- (Exam Topic 3)

Which of the following BEST indicates whether security awareness training is effective?

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

Answer: B

NEW QUESTION 215

- (Exam Topic 3)

Which of the following should be management's PRIMARY focus when key risk indicators (KRIs) begin to rapidly approach defined thresholds?

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

Answer: D

NEW QUESTION 219

- (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 220

- (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 221

- (Exam Topic 3)

Which of the following would BEST help an enterprise define and communicate its risk appetite?

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

Answer: C

NEW QUESTION 222

- (Exam Topic 3)

Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information to a supplier?

- A. Encrypt the data while in transit to 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 227

- (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 228

- (Exam Topic 3)

Which of the following is the PRIMARY reason to use key control indicators (KCI) to evaluate control operating effectiveness?

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

Answer: C

NEW QUESTION 232

- (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 235

- (Exam Topic 3)

Which of the following roles is BEST suited to help a risk practitioner understand the impact of IT-related events on business objectives?

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

Answer: C

NEW QUESTION 238

- (Exam Topic 3)

Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:

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

Answer: D

NEW QUESTION 242

- (Exam Topic 3)

A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

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

Answer: D

NEW QUESTION 245

- (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 248

- (Exam Topic 3)

Which of the following is the MOST important reason to link an effective key control indicator (KCI) to relevant key risk indicators (KRIs)?

- A. To monitor changes in the risk environment
- B. To provide input to management for the adjustment of risk appetite
- C. To monitor the accuracy of threshold levels in metrics
- D. To obtain business buy-in for investment in risk mitigation measures

Answer: A

NEW QUESTION 249

- (Exam Topic 3)

Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?

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

Answer: B

NEW QUESTION 253

- (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 257

- (Exam Topic 3)

Which of the following would BEST assist in reconstructing the sequence of events following a security incident across multiple IT systems in the organization's network?

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

Answer: D

NEW QUESTION 260

- (Exam Topic 3)

Which of the following would present the MOST significant risk to an organization when updating the incident response plan?

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

Answer: D

NEW QUESTION 265

- (Exam Topic 3)

Which of the following key control indicators (KCIs) BEST indicates whether security requirements are identified and managed throughout a project life cycle?

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

Answer: A

NEW QUESTION 266

- (Exam Topic 3)

Which of the following is the BEST reason to use qualitative measures to express residual risk levels related to emerging threats?

- A. Qualitative measures require less ongoing monitoring.
- B. Qualitative measures are better aligned to regulatory requirements.
- C. Qualitative measures are better able to incorporate expert judgment.
- D. Qualitative measures are easier to update.

Answer: C

NEW QUESTION 269

- (Exam Topic 3)

An organization is conducting a review of emerging risk. Which of the following is the BEST input for this exercise?

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

Answer: B

NEW QUESTION 270

- (Exam Topic 3)

Which of the following would be MOST helpful to a risk practitioner when ensuring that mitigated risk remains within acceptable limits?

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

Answer: D

NEW QUESTION 272

- (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)

Key risk indicators (KRIs) are MOST useful during which of the following risk management phases?

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

Answer: A

NEW QUESTION 276

- (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 279

- (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 281

- (Exam Topic 3)

When reviewing a business continuity plan (BCP), which of the following would be the MOST significant deficiency?

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

Answer: B

NEW QUESTION 283

- (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 284

- (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 286

- (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 290

- (Exam Topic 3)

The PRIMARY advantage of involving end users in continuity planning is that they:

- A. have a better understanding of specific business needs
- B. can balance the overall technical and business concerns
- C. can see the overall impact to the business
- D. are more objective than information security management.

Answer: B

NEW QUESTION 292

- (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 297

- (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 300

- (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 302

- (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 303

- (Exam Topic 3)

Which of the following is MOST important to compare against the corporate risk profile?

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

Answer: D

NEW QUESTION 307

- (Exam Topic 3)

Which of the following would be MOST useful to senior management when determining an appropriate risk response?

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

Answer: A

NEW QUESTION 311

- (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 316

- (Exam Topic 3)

Which of the following BEST facilitates 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 319

- (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 322

- (Exam Topic 3)

Which of the following approaches BEST identifies information systems control deficiencies?

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

Answer: C

NEW QUESTION 327

- (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 330

- (Exam Topic 3)

Which of The following is the MOST comprehensive input to the risk assessment process specific to the effects of system downtime?

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

Answer: C

NEW QUESTION 334

- (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 337

- (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 338

- (Exam Topic 3)

A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

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

Answer: B

NEW QUESTION 342

- (Exam Topic 3)

Which of the following is the BEST source for identifying key control indicators (KCIs)?

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

Answer: B

NEW QUESTION 344

- (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 349

- (Exam Topic 3)

Days before the realization of an acquisition, a data breach is discovered at the company to be acquired. For the accruing organization, this situation represents which of the following?

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

Answer: B

NEW QUESTION 352

- (Exam Topic 3)

Which of the following BEST enforces access control for an organization that uses multiple cloud technologies?

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

Answer: C

NEW QUESTION 354

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 358

- (Exam Topic 3)

Print jobs containing confidential information are sent to a shared network printer located in a secure room. Which of the following is the BEST control to prevent the inappropriate disclosure of confidential information?

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

Answer: A

NEW QUESTION 361

- (Exam Topic 3)

A deficient control has been identified which could result in great harm to an organization should a low frequency threat event occur. When communicating the associated risk to senior management the risk practitioner should explain:

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

Answer: A

NEW QUESTION 362

- (Exam Topic 3)

Which of The following should be the FIRST step when a company is made aware of new regulatory requirements impacting IT?

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

Answer: C

NEW QUESTION 364

- (Exam Topic 3)

In an organization where each division manages risk independently, which of the following would BEST enable management of risk at the enterprise level?

- A. A standardized risk taxonomy
- B. A list of control deficiencies
- C. An enterprise risk ownership policy
- D. An updated risk tolerance metric

Answer: A

NEW QUESTION 366

- (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 368

- (Exam Topic 4)

Senior management is deciding whether to share confidential data with the organization's business partners. The BEST course of action for a risk practitioner would be to submit a report to senior management containing the:

- A. possible risk and suggested mitigation plans.
- B. design of controls to encrypt the data to be shared.
- C. project plan for classification of the data.
- D. summary of data protection and privacy legislation.

Answer: A

NEW QUESTION 372

- (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 376

- (Exam Topic 4)

A company has recently acquired a customer relationship management (CRM) application from a certified software vendor. Which of the following will BEST help to prevent technical vulnerabilities from being exploited?

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

Answer: D

NEW QUESTION 378

- (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 383

- (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 388

- (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 390

- (Exam Topic 4)

An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

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

Answer: A

NEW QUESTION 395

- (Exam Topic 4)

Which of the following provides the MOST useful information to assess the magnitude of identified deficiencies in the IT control environment?

- A. Peer benchmarks
- B. Internal audit reports
- C. Business impact analysis (BIA) results
- D. Threat analysis results

Answer: D

NEW QUESTION 398

- (Exam Topic 4)

Which of the following BEST enables senior management to 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 402

- (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 404

- (Exam Topic 4)

Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

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

Answer: D

NEW QUESTION 409

- (Exam Topic 4)

Which of the following would BEST facilitate the implementation of data classification requirements?

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

Answer: A

NEW QUESTION 414

- (Exam Topic 4)

Which of the following sources is MOST relevant to reference when updating security awareness training materials?

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

Answer: B

NEW QUESTION 417

- (Exam Topic 4)

A recent vulnerability assessment of a web-facing application revealed several weaknesses. Which of the following should be done NEXT to determine the risk exposure?

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

Answer: B

NEW QUESTION 420

- (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 425

- (Exam Topic 4)

Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

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

Answer: B

NEW QUESTION 426

- (Exam Topic 4)

Which of the following would be a risk practitioner's BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

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

Answer: A

NEW QUESTION 427

- (Exam Topic 4)

Which of the following potential scenarios associated with the implementation of a new database technology presents the GREATEST risk to an organization?

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

Answer: B

NEW QUESTION 431

- (Exam Topic 4)

Which of the following is the PRIMARY reason for sharing risk assessment reports with senior stakeholders?

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

Answer: A

NEW QUESTION 432

- (Exam Topic 4)

Which of the following will BEST help to ensure key risk indicators (KRIs) provide value to risk owners?

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

Answer: B

NEW QUESTION 435

- (Exam Topic 4)

Which of the following is the MOST effective way to identify an application backdoor prior to implementation?

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

Answer: B

NEW QUESTION 439

- (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 442

- (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 444

- (Exam Topic 4)

Which of the following is the PRIMARY objective of risk management?

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

Answer: B

NEW QUESTION 449

- (Exam Topic 4)

Who is MOST important to include in the assessment of existing IT risk scenarios?

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

Answer: C

NEW QUESTION 454

- (Exam Topic 4)

An organization wants to grant remote access to a system containing sensitive data to an overseas third party. Which of the following should be of GREATEST concern to management?

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

Answer: C

NEW QUESTION 458

- (Exam Topic 4)

Which of the following should be used as the PRIMARY basis for evaluating the state of an organization's cloud computing environment against leading practices?

- A. The cloud environment's capability maturity model
- B. The cloud environment's risk register
- C. The cloud computing architecture
- D. The organization's strategic plans for cloud computing

Answer: A

NEW QUESTION 463

- (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 465

- (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 469

- (Exam Topic 4)

Which of the following is the MAIN purpose of monitoring risk?

- A. Communication
- B. Risk analysis
- C. Decision support
- D. Benchmarking

Answer: A

NEW QUESTION 471

- (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 472

- (Exam Topic 4)

Which of the following would BEST mitigate an identified risk scenario?

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

Answer: C

NEW QUESTION 477

- (Exam Topic 4)

Which of the following would be a risk practitioner's BEST course of action when a project team has accepted a risk outside the established risk appetite?

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

Answer: B

NEW QUESTION 479

- (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 481

- (Exam Topic 4)

To define the risk management strategy which of the following MUST be set by the board of directors?

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

Answer: B

NEW QUESTION 485

- (Exam Topic 4)

Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

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

Answer: A

NEW QUESTION 490

- (Exam Topic 4)

Which of the following is the MOST important outcome of a business impact analysis (BIA)?

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

Answer: A

NEW QUESTION 492

- (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 496

- (Exam Topic 4)

Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

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

Answer: A

NEW QUESTION 500

- (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 503

- (Exam Topic 4)

Which of the following is the PRIMARY reason to engage business unit managers in risk management processes'?

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

Answer: C

NEW QUESTION 504

- (Exam Topic 4)

Which of the following BEST facilitates the identification of appropriate key performance indicators (KPIs) for a risk management program?

- A. Reviewing control objectives
- B. Aligning with industry best practices
- C. Consulting risk owners
- D. Evaluating KPIs in accordance with risk appetite

Answer: C

NEW QUESTION 507

- (Exam Topic 4)

When defining thresholds for control key performance indicators (KPIs), it is MOST helpful to align:

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

Answer: B

NEW QUESTION 509

- (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 contract

Answer: A

NEW QUESTION 510

- (Exam Topic 4)

Which of the following is the GREATEST benefit of centralizing IT systems?

- A. Risk reporting
- B. Risk classification
- C. Risk monitoring
- D. Risk identification

Answer: C

NEW QUESTION 514

- (Exam Topic 4)

An organization has experienced several incidents of extended network outages that have exceeded tolerance. Which of the following should be the risk practitioner's FIRST step to address this situation?

- A. Recommend additional controls to address the risk.
- B. Update the risk tolerance level to acceptable thresholds.
- C. Update the incident-related risk trend in the risk register.
- D. Recommend a root cause analysis of the incidents.

Answer: D

NEW QUESTION 519

- (Exam Topic 4)

An organization has been experiencing an increasing number of spear phishing attacks Which of the following would be the MOST effective way to mitigate the risk associated with these attacks?

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

Answer: A

NEW QUESTION 521

- (Exam Topic 4)

A risk practitioner is reviewing accountability assignments for data risk in the risk register. Which of the following would pose the GREATEST concern?

- A. The risk owner is not the control owner for associated data controls.
- B. The risk owner is in a business unit and does not report through the IT department.
- C. The risk owner is listed as the department responsible for decision making.
- D. The risk owner is a staff member rather than a department manager.

Answer: C

NEW QUESTION 526

- (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 527

- (Exam Topic 4)

The cost of maintaining a control has grown to exceed the potential loss. Which of the following BEST describes this situation?

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

Answer: B

NEW QUESTION 531

- (Exam Topic 4)

Which of the following is the BEST approach for selecting controls to minimize risk?

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

Answer: C

NEW QUESTION 533

- (Exam Topic 4)

Which of the following is MOST helpful in providing a high-level overview of current IT risk severity*?

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

Answer: B

NEW QUESTION 534

- (Exam Topic 4)

Which of the following provides the MOST reliable evidence of a control's effectiveness?

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

Answer: D

NEW QUESTION 538

- (Exam Topic 4)

Which of the following would be the BEST way for a risk practitioner to validate the effectiveness of a patching program?

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

Answer: C

NEW QUESTION 539

- (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 540

- (Exam Topic 4)

An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

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

Answer: A

NEW QUESTION 545

- (Exam Topic 4)

A risk practitioner has established that a particular control is working as desired, but the annual cost of maintenance has increased and now exceeds the expected annual loss exposure. The result is that the control is:

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

Answer: B

NEW QUESTION 547

- (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 552

- (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 554

- (Exam Topic 4)

Which of the following should be accountable for ensuring that media containing financial information are adequately destroyed per an organization's data disposal policy?

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

Answer: C

NEW QUESTION 558

- (Exam Topic 4)

Who should be responsible for determining which stakeholders need to be involved in the development of a risk scenario?

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

Answer: B

NEW QUESTION 563

- (Exam Topic 4)

Which of the following would present the GREATEST challenge for a risk practitioner during a merger of two organizations?

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

Answer: A

NEW QUESTION 566

- (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 571

- (Exam Topic 4)

Which of the following is the GREATEST benefit of identifying appropriate risk owners?

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

Answer: A

NEW QUESTION 573

- (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 578

- (Exam Topic 4)

Which of the following is the GREATEST benefit of a three lines of defense structure?

- A. An effective risk culture that empowers employees to report risk
- B. Effective segregation of duties to prevent internal fraud
- C. Clear accountability for risk management processes
- D. Improved effectiveness and efficiency of business operations

Answer: C

NEW QUESTION 582

- (Exam Topic 4)

The MAIN purpose of selecting a risk response is to.

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

Answer: C

NEW QUESTION 585

- (Exam Topic 4)

Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?

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

Answer: D

NEW QUESTION 587

- (Exam Topic 4)

What should be the PRIMARY consideration related to data privacy protection when there are plans for a business initiative to make use of personal information?

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

Answer: D

NEW QUESTION 591

- (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 595

- (Exam Topic 4)

Which of the following should be a risk practitioner's NEXT step after learning of an incident that has affected a competitor?

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

Answer: A

NEW QUESTION 597

- (Exam Topic 4)

Which of the following would BEST mitigate the ongoing risk associated with operating system (OS) vulnerabilities?

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

Answer: B

NEW QUESTION 601

- (Exam Topic 4)

An internal audit report reveals that a legacy system is no longer supported Which of the following is the risk practitioner's MOST important action before recommending a risk response'

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

Answer: B

NEW QUESTION 602

- (Exam Topic 4)

The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.

Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading to data compromise	Risk Council	End-User Computing Manager AND Inventory	IT Operations Manager AND Security Operations Manager	Low Likelihood	Very Serious	0.120	Mitigate	Purchase and acquire data encryption software for mobile devices
R003	Fire Hazard	A fire accident may destroy data center equipment and servers leading to loss of availability and services	Information Security Department	Data Center Facilities Manager	Facilities Manager	Low Likelihood	Serious	0.060	Transfer	Buy fire hazard insurance policy
		A disgruntled								
		Significant				0.10	Low Likelihood			0.30
		Serious				0.20	Likely			0.50
		Very Serious				0.40	Highly Likely			0.70
		Catastrophic				0.80	Near Certainty			0.90

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

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

Answer: B

NEW QUESTION 607

- (Exam Topic 4)

Which of the following is MOST important for an organization to consider when developing its IT strategy?

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

Answer: C

NEW QUESTION 612

- (Exam Topic 3)

Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

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

Answer: C

NEW QUESTION 617

- (Exam Topic 3)

A risk practitioner has discovered a deficiency in a critical system that cannot be patched. Which of the following should be the risk practitioner's FIRST course of action?

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

Answer: C

NEW QUESTION 620

- (Exam Topic 3)

Upon learning that the number of failed back-up attempts continually exceeds the current risk threshold, the risk practitioner should:

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

Answer: D

NEW QUESTION 623

- (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 626

- (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 627

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 630

- (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 633

- (Exam Topic 3)

Which element of an organization's risk register is MOST important to update following the commissioning of a new financial reporting system?

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

Answer: C

NEW QUESTION 634

- (Exam Topic 3)

Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

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

Answer: C

NEW QUESTION 636

- (Exam Topic 3)

Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

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

Answer: A

NEW QUESTION 639

- (Exam Topic 3)

Which of the following is the MOST effective control to ensure user access is maintained on a least-privilege basis?

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

Answer: B

NEW QUESTION 644

- (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 649

- (Exam Topic 3)

Who should be PRIMARILY responsible for establishing an organization's IT risk culture?

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

Answer: B

NEW QUESTION 653

- (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 656

- (Exam Topic 3)

An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

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

Answer: D

NEW QUESTION 657

- (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 661

- (Exam Topic 3)

The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

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

Answer: D

NEW QUESTION 663

- (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 664

- (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 668

- (Exam Topic 3)

Which of the following is the BEST indicator of an effective IT security awareness program?

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

Answer: A

NEW QUESTION 671

- (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 674

- (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 679

- (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 683

- (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 684

- (Exam Topic 3)

Which of the following is the BEST way to assess the effectiveness of an access management process?

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

Answer: B

NEW QUESTION 687

- (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 692

- (Exam Topic 3)

Which of the following is MOST important when developing risk scenarios?

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

Answer: D

NEW QUESTION 696

- (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 698

- (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 701

- (Exam Topic 3)

Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?

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

Answer: A

NEW QUESTION 702

- (Exam Topic 3)

Which of the following is a drawback in the use of quantitative risk analysis?

- A. It assigns numeric values to exposures of assets.
- B. It requires more resources than other methods
- C. It produces the results in numeric form.
- D. It is based on impact analysis of information assets.

Answer: B

NEW QUESTION 707

- (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 708

- (Exam Topic 3)

In an organization that allows employee use of social media accounts for work purposes, which of the following is the BEST way to protect company sensitive information from being exposed?

- A. Educating employees on what needs to be kept confidential
- B. Implementing a data loss prevention (DLP) solution
- C. Taking punitive action against employees who expose confidential data
- D. Requiring employees to sign nondisclosure agreements

Answer: B

NEW QUESTION 713

- (Exam Topic 3)

In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

- A. two-factor authentication.
- B. continuous data backup controls.
- C. encryption for data at rest.
- D. encryption for data in motion.

Answer: B

NEW QUESTION 717

- (Exam Topic 3)

Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?

- A. Unknown vulnerabilities
- B. Legacy technology systems
- C. Network isolation
- D. Overlapping threats

Answer: D

NEW QUESTION 722

- (Exam Topic 3)

The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

- A. assess gaps in IT risk management operations and strategic focus.
- B. confirm that IT risk assessment results are expressed as business impact.
- C. verify implemented controls to reduce the likelihood of threat materialization.
- D. ensure IT risk management is focused on mitigating potential risk.

Answer: D

NEW QUESTION 724

- (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 727

- (Exam Topic 3)

An IT control gap has been identified in a key process. Who would be the MOST appropriate owner of the risk associated with this gap?

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

Answer: A

NEW QUESTION 732

- (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 733

- (Exam Topic 3)

Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

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

Answer: A

NEW QUESTION 735

- (Exam Topic 3)

An organization is implementing encryption for data at rest to reduce the risk associated with unauthorized access. Which of the following MUST be considered to assess the residual risk?

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

Answer: D

NEW QUESTION 739

- (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 743

- (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 748

- (Exam Topic 3)

Which of the following presents the GREATEST risk to change control in business application development over the complete life cycle?

- A. Emphasis on multiple application testing cycles
- B. Lack of an integrated development environment (IDE) tool
- C. Introduction of requirements that have not been approved
- D. Bypassing quality requirements before go-live

Answer: C

NEW QUESTION 749

- (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 750

- (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 754

- (Exam Topic 3)

While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially. Which of the following would be the BEST approach for the risk practitioner to take?

- A. Temporarily suspend emergency changes.
- B. Document the control deficiency in the risk register.
- C. Conduct a root cause analysis.
- D. Continue monitoring change management metrics.

Answer: C

NEW QUESTION 759

- (Exam Topic 3)

Accountability for a particular risk is BEST represented in a:

- A. risk register
- B. risk catalog

- C. risk scenario
- D. RACI matrix

Answer: D

NEW QUESTION 761

- (Exam Topic 3)

Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (AI) solutions into the organization?

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

Answer: B

NEW QUESTION 762

- (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 765

- (Exam Topic 2)

The PRIMARY reason for establishing various Threshold levels for a set of key risk indicators (KRIs) is to:

- A. highlight trends of developing risk.
- B. ensure accurate and reliable monitoring.
- C. take appropriate actions in a timely manner.
- D. set different triggers for each stakeholder.

Answer: B

NEW QUESTION 770

- (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 775

- (Exam Topic 2)

When reviewing a risk response strategy, senior management's PRIMARY focus should be placed on the:

- A. cost-benefit analysis.
- B. investment portfolio.
- C. key performance indicators (KPIs).
- D. alignment with risk appetite.

Answer: D

NEW QUESTION 778

- (Exam Topic 2)

Mapping open risk issues to an enterprise risk heat map BEST facilitates:

- A. risk response.
- B. control monitoring.
- C. risk identification.
- D. risk ownership.

Answer: A

NEW QUESTION 780

- (Exam Topic 2)

A risk practitioner has just learned about new done FIRST?

- A. Notify executive management.
- B. Analyze the impact to the organization.
- C. Update the IT risk register.
- D. Design IT risk mitigation plans.

Answer: B

NEW QUESTION 784

- (Exam Topic 2)

Which of the following **MUST** be assessed before considering risk treatment options for a scenario with significant impact?

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

Answer: D

NEW QUESTION 787

- (Exam Topic 2)

A bank is experiencing an increasing incidence of customer identity theft. Which of the following is the **BEST** way to mitigate this risk?

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

Answer: B

NEW QUESTION 788

- (Exam Topic 2)

Which of the following is **MOST** commonly compared against the risk appetite?

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

Answer: D

NEW QUESTION 791

- (Exam Topic 2)

Who is accountable for risk treatment?

- A. Enterprise risk management team
- B. Risk mitigation manager
- C. Business process owner
- D. Risk owner

Answer: D

NEW QUESTION 793

- (Exam Topic 2)

When reporting risk assessment results to senior management, which of the following is **MOST** important to include to enable risk-based decision making?

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

Answer: A

NEW QUESTION 797

- (Exam Topic 2)

Which of the following is a detective control?

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

Answer: B

NEW QUESTION 800

- (Exam Topic 2)

Which of the following provides the MOST helpful information in identifying risk in an organization?

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

Answer: C

NEW QUESTION 802

- (Exam Topic 2)

After migrating a key financial system to a new provider, it was discovered that a developer could gain access to the production environment. Which of the following is the BEST way to mitigate the risk in this situation?

- A. Escalate the issue to the service provider.
- B. Re-certify the application access controls.
- C. Remove the developer's access.
- D. Review the results of pre-migration testing.

Answer: B

NEW QUESTION 805

- (Exam Topic 2)

Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?

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

Answer: D

NEW QUESTION 809

- (Exam Topic 2)

Which of the following resources is MOST helpful when creating a manageable set of IT risk scenarios?

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

Answer: B

NEW QUESTION 813

- (Exam Topic 2)

Which of the following conditions presents the GREATEST risk to an application?

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

Answer: D

NEW QUESTION 817

- (Exam Topic 2)

The PRIMARY purpose of a maturity model is to compare the:

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

Answer: A

NEW QUESTION 822

- (Exam Topic 2)

Due to a change in business processes, an identified risk scenario no longer requires mitigation. Which of the following is the MOST important reason the risk should remain in the risk register?

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

Answer: C

NEW QUESTION 827

- (Exam Topic 2)

An organization is considering modifying its system to enable acceptance of credit card payments. To reduce the risk of data exposure, which of the following should the organization do FIRST?

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

Answer: A

NEW QUESTION 830

- (Exam Topic 2)

Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is aligned to business requirements?

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

Answer: C

NEW QUESTION 834

- (Exam Topic 2)

An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

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

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

Answer: A

NEW QUESTION 839

- (Exam Topic 2)

An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

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

Answer: D

NEW QUESTION 842

- (Exam Topic 2)

Which of the following will BEST ensure that information security risk factors are mitigated when developing in-house applications?

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

Answer: D

NEW QUESTION 846

- (Exam Topic 2)

A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

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

Answer: A

NEW QUESTION 851

- (Exam Topic 2)

A risk practitioner has learned that an effort to implement a risk mitigation action plan has stalled due to lack of funding. The risk practitioner should report that the associated risk has been:

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

Answer: B

NEW QUESTION 853

- (Exam Topic 2)

Which of the following BEST helps to balance the costs and benefits of managing IT risk?

- A. Prioritizing risk responses
- B. Evaluating risk based on frequency and probability
- C. Considering risk factors that can be quantified
- D. Managing the risk by using controls

Answer: A

NEW QUESTION 858

- (Exam Topic 2)

Which of these documents is MOST important to request from a cloud service provider during a vendor risk assessment?

- A. Nondisclosure agreement (NDA)
- B. Independent audit report
- C. Business impact analysis (BIA)
- D. Service level agreement (SLA)

Answer: B

NEW QUESTION 863

- (Exam Topic 2)

Which of the following is MOST influential when management makes risk response decisions?

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

Answer: A

NEW QUESTION 865

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?

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

Answer: D

NEW QUESTION 866

- (Exam Topic 2)

Which of the following should be the PRIMARY focus of an independent review of a risk management process?

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

Answer: B

NEW QUESTION 869

- (Exam Topic 2)

The GREATEST concern when maintaining a risk register is that:

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

Answer:

D

NEW QUESTION 871

- (Exam Topic 2)

The PRIMARY purpose of using control metrics is to evaluate the:

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

Answer: C

NEW QUESTION 872

- (Exam Topic 2)

Which of the following would be a weakness in procedures for controlling the migration of changes to production libraries?

- A. The programming project leader solely reviews test results before approving the transfer to production.
- B. Test and production programs are in distinct libraries.
- C. Only operations personnel are authorized to access production libraries.
- D. A synchronized migration of executable and source code from the test environment to the production environment is allowed.

Answer: A

NEW QUESTION 877

- (Exam Topic 2)

Which of the following would MOST likely cause a risk practitioner to reassess risk scenarios?

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

Answer: C

NEW QUESTION 878

- (Exam Topic 2)

It is MOST important for a risk practitioner to have an awareness of an organization's processes in order to:

- A. perform a business impact analysis.
- B. identify potential sources of risk.
- C. establish risk guidelines.
- D. understand control design.

Answer: B

NEW QUESTION 880

- (Exam Topic 2)

Which of the following BEST enables the risk profile to serve as an effective resource to support business objectives?

- A. Engaging external risk professionals to periodically review the risk
- B. Prioritizing global standards over local requirements in the risk profile
- C. Updating the risk profile with risk assessment results
- D. Assigning quantitative values to qualitative metrics in the risk register

Answer: C

NEW QUESTION 885

- (Exam Topic 2)

Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

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

Answer: D

NEW QUESTION 886

- (Exam Topic 2)

Which of the following can be interpreted from a single data point on a risk heat map?

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

Answer: B

NEW QUESTION 890

- (Exam Topic 2)

What are the MOST important criteria to consider when developing a data classification scheme to facilitate risk assessment and the prioritization of risk mitigation activities?

- A. Mitigation and control value
- B. Volume and scope of data generated daily
- C. Business criticality and sensitivity
- D. Recovery point objective (RPO) and recovery time objective (RTO)

Answer: C

NEW QUESTION 892

- (Exam Topic 2)

When testing the security of an IT system, it is MOST important to ensure that;

- A. tests are conducted after business hours.
- B. operators are unaware of the test.
- C. external experts execute the test.
- D. agreement is obtained from stakeholders.

Answer: D

NEW QUESTION 895

- (Exam Topic 2)

What can be determined from the risk scenario chart?

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

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

Answer: A

NEW QUESTION 896

- (Exam Topic 2)

Which of the following provides the MOST important information to facilitate a risk response decision?

- A. Audit findings
- B. Risk appetite
- C. Key risk indicators
- D. Industry best practices

Answer: B

NEW QUESTION 900

- (Exam Topic 2)

An organization's risk tolerance should be defined and approved by which of the following?

- A. The chief risk officer (CRO)
- B. The board of directors
- C. The chief executive officer (CEO)
- D. The chief information officer (CIO)

Answer: B

NEW QUESTION 904

- (Exam Topic 2)

As part of an overall IT risk management plan, an IT risk register BEST helps management:

- A. align IT processes with business objectives.
- B. communicate the enterprise risk management policy.
- C. stay current with existing control status.
- D. understand the organizational risk profile.

Answer: D

NEW QUESTION 907

- (Exam Topic 2)

Which of the following will BEST help to ensure that information system controls are effective?

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

Answer: C

NEW QUESTION 910

- (Exam Topic 2)

The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

- A. ensure policy and regulatory compliance.
- B. assess the proliferation of new threats.
- C. verify Internet firewall control settings.
- D. identify vulnerabilities in the system.

Answer: C

NEW QUESTION 915

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CRISC Practice Exam Features:

- * CRISC Questions and Answers Updated Frequently
- * CRISC Practice Questions Verified by Expert Senior Certified Staff
- * CRISC Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CRISC Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CRISC Practice Test Here](#)