



Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 4)

What is the MAIN benefit of using a top-down approach to develop risk scenarios?

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

Answer: C

NEW QUESTION 2

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 3

- (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 4

- (Exam Topic 4)

Which of the following should be the GREATEST concern to a risk practitioner when process documentation is incomplete?

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

Answer: B

NEW QUESTION 5

- (Exam Topic 4)

A highly regulated enterprise is developing a new risk management plan to specifically address legal and regulatory risk scenarios What should be done FIRST by IT governance to support this effort?

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

Answer: A

NEW QUESTION 6

- (Exam Topic 4)

Which of the following is the 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 7

- (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 8

- (Exam Topic 4)

An organization's business gap analysis reveals the need for a robust IT risk strategy. Which of the following should be the risk practitioner's PRIMARY consideration when participating in development of the new strategy?

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

Answer: C

NEW QUESTION 9

- (Exam Topic 4)

Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 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 is the MOST important information to cover a business continuity awareness training program for all employees of the organization?

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

Answer: C

NEW QUESTION 11

- (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 12

- (Exam Topic 4)

When a risk practitioner is determining a system's criticality, it is MOST helpful to review the associated:

- A. process flow.
- B. business impact analysis (BIA).
- C. service level agreement (SLA).
- D. system architecture.

Answer: B

NEW QUESTION 14

- (Exam Topic 4)

Risk appetite should be PRIMARILY driven by which of the following?

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

Answer: B

NEW QUESTION 15

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 18

- (Exam Topic 4)

Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

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

Answer: A

NEW QUESTION 23

- (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 26

- (Exam Topic 4)

Which of the following provides the MOST useful information for developing key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 27

- (Exam Topic 4)

An organization's control environment is MOST effective when:

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

Answer: A

NEW QUESTION 32

- (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 35

- (Exam Topic 4)

Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?

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

Answer: B

NEW QUESTION 36

- (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 37

- (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 38

- (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 43

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 47

- (Exam Topic 4)

Which of the following practices would be MOST effective in protecting personally identifiable information (PII) from unauthorized access in a cloud environment?

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

Answer: B

NEW QUESTION 50

- (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 activities
- B. The maximum levels of applicable regulatory fines
- C. The length of time between identification and containment of the incident
- D. The composition and number of records in the information asset

Answer:

C

NEW QUESTION 55

- (Exam Topic 4)

In order to determining a risk is under-controlled the risk practitioner will need to

- A. understand the risk tolerance
- B. monitor and evaluate IT performance
- C. identify risk management best practices
- D. determine the sufficiency of the IT risk budget

Answer: A

NEW QUESTION 56

- (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 57

- (Exam Topic 4)

An organization has asked an IT risk practitioner to conduct an operational risk assessment on an initiative to outsource the organization's customer service operations overseas. Which of the following would MOST significantly impact management's decision?

- A. Time zone difference of the outsourcing location
- B. Ongoing financial viability of the outsourcing company
- C. Cross-border information transfer restrictions in the outsourcing country
- D. Historical network latency between the organization and outsourcing location

Answer: C

NEW QUESTION 61

- (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 65

- (Exam Topic 4)

Which of the following is MOST likely to introduce risk for financial institutions that use blockchain?

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

Answer: B

NEW QUESTION 66

- (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 67

- (Exam Topic 4)

Which of The following BEST represents the desired risk posture for an organization?

- A. Inherent risk is lower than risk tolerance.

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

Answer: D

NEW QUESTION 70

- (Exam Topic 4)

Which of the following is the BEST way to validate whether controls to reduce user device vulnerabilities have been implemented according to management's action plan?

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

Answer: B

NEW QUESTION 75

- (Exam Topic 4)

A MAJOR advantage of using key risk indicators (KRIs) is that they

- 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 appetite

Answer: B

NEW QUESTION 77

- (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 identify all relevant issues.
- B. be too costly
- C. violate laws in other countries
- D. be too time consuming

Answer: C

NEW QUESTION 79

- (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 82

- (Exam Topic 3)

The PRIMARY reason for prioritizing risk scenarios is to:

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

Answer: D

NEW QUESTION 85

- (Exam Topic 4)

Which of the following management actions will MOST likely change the likelihood rating of a risk scenario related to remote network access?

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

Answer: A

NEW QUESTION 89

- (Exam Topic 4)

A penetration test reveals several vulnerabilities in a web-facing application. Which of the following should be the FIRST step in selecting a risk response?

- A. Correct the vulnerabilities to mitigate potential risk exposure.
- B. Develop a risk response action plan with key stakeholders.
- C. Assess the level of risk associated with the vulnerabilities.
- D. Communicate the vulnerabilities to the risk owner.

Answer: C

NEW QUESTION 91

- (Exam Topic 4)

Which of the following is MOST important to consider before determining a response to a vulnerability?

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

Answer: C

NEW QUESTION 94

- (Exam Topic 4)

A legacy application used for a critical business function relies on software that has reached the end of extended support Which of the following is the MOST effective control to manage this application?

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

Answer: D

NEW QUESTION 96

- (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 101

- (Exam Topic 3)

An organization has implemented a preventive control to lock user accounts after three unsuccessful login attempts. This practice has been proven to be unproductive, and a change in the control threshold value has been recommended. Who should authorize changing this threshold?

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

Answer: D

NEW QUESTION 103

- (Exam Topic 3)

Which of the following statements describes the relationship between key risk indicators (KRIs) and key control indicators (KCIs)?

- A. KRI design must precede definition of KCIs.
- B. KCIs and KRIs are independent indicators and do not impact each other.
- C. A decreasing trend of KRI readings will lead to changes to KCIs.
- D. Both KRIs and KCIs provide insight to potential changes in the level of risk.

Answer: A

NEW QUESTION 106

- (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 107

- (Exam Topic 3)

Which of the following is MOST useful when communicating risk to management?

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

Answer: C

NEW QUESTION 108

- (Exam Topic 3)

During a risk treatment plan review, a risk practitioner finds the approved risk action plan has not been completed. However, there were other risk mitigation actions implemented. Which of the following is the BEST course of action?

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

Answer: A

NEW QUESTION 110

- (Exam Topic 3)

The MAIN reason for creating and maintaining a risk register is to:

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

Answer: D

NEW QUESTION 115

- (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 119

- (Exam Topic 3)

Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?

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

Answer: D

NEW QUESTION 121

- (Exam Topic 3)

When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

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

Answer: D

NEW QUESTION 122

- (Exam Topic 3)

Which of the following controls are BEST strengthened by a clear organizational code of ethics?

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

Answer: B

NEW QUESTION 124

- (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 127

- (Exam Topic 3)

Which of the following is the MOST important objective of establishing an enterprise risk management (ERM) function within an organization?

- A. To have a unified approach to risk management across the organization
- B. To have a standard risk management process for complying with regulations
- C. To optimize risk management resources across the organization
- D. To ensure risk profiles are presented in a consistent format within the organization

Answer: A

NEW QUESTION 128

- (Exam Topic 3)

Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

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

Answer: C

NEW QUESTION 131

- (Exam Topic 3)

Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

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

Answer: B

NEW QUESTION 134

- (Exam Topic 3)

Which of the following should be considered when selecting a risk response?

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

Answer: B

NEW QUESTION 135

- (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 138

- (Exam Topic 3)

Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

- A. Key performance indicators (KPIs)
- B. Risk heat maps

- C. Internal audit findings
- D. Periodic penetration testing

Answer: A

NEW QUESTION 139

- (Exam Topic 3)

The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:

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

Answer: B

NEW QUESTION 144

- (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 149

- (Exam Topic 3)

Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?

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

Answer: D

NEW QUESTION 153

- (Exam Topic 3)

Several network user accounts were recently created without the required management approvals. Which of the following would be the risk practitioner's BEST recommendation to address this situation?

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

Answer: C

NEW QUESTION 154

- (Exam Topic 3)

When of the following is the BEST key control indicator (KCI) to determine the effectiveness of an intrusion prevention system (IPS)?

- A. Percentage of system uptime
- B. Percentage of relevant threats mitigated
- C. Total number of threats identified
- D. Reaction time of the system to threats

Answer: B

NEW QUESTION 157

- (Exam Topic 3)

A service provider is managing a client's servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider's MOST appropriate action would be to:

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

Answer: D

NEW QUESTION 161

- (Exam Topic 3)

Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

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

Answer: C

NEW QUESTION 165

- (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 168

- (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 171

- (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 176

- (Exam Topic 3)

Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

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

Answer: C

NEW QUESTION 180

- (Exam Topic 3)

Which of the following is MOST important when developing key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 183

- (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 186

- (Exam Topic 3)

Which of the following BEST indicates the condition of a risk management program?

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

Answer: D

NEW QUESTION 191

- (Exam Topic 3)

Which of the following is the BEST indication of a mature organizational risk culture?

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

Answer: B

NEW QUESTION 192

- (Exam Topic 3)

When of the following provides the MOST tenable evidence that a business process control is effective?

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

Answer: C

NEW QUESTION 194

- (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 197

- (Exam Topic 3)

Which of the following should be the PRIMARY goal of developing information security metrics?

- A. Raising security awareness
- B. Enabling continuous improvement
- C. Identifying security threats
- D. Ensuring regulatory compliance

Answer: B

NEW QUESTION 202

- (Exam Topic 3)

An organization has been notified that a disgruntled, terminated IT administrator has tried to break into the corporate network. Which of the following discoveries should be of GREATEST concern to the organization?

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

Answer: A

NEW QUESTION 203

- (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 207

- (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 211

- (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 216

- (Exam Topic 3)

Which of the following is the MOST significant exposure when an application uses individual user accounts to access the underlying database?

- A. Users may share accounts with business system analyst
- B. Application may not capture a complete audit trail.
- C. Users may be able to circumvent application controls.
- D. Multiple connects to the database are used and slow the process

Answer: C

NEW QUESTION 220

- (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 222

- (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 226

- (Exam Topic 3)

Which of the following should be the risk practitioner's FIRST course of action when an organization plans to adopt a cloud computing strategy?

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

Answer: B

NEW QUESTION 228

- (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 229

- (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 233

- (Exam Topic 3)

Who should have the authority to approve an exception to a control?

- A. information security manager
- B. Control owner
- C. Risk owner
- D. Risk manager

Answer: C

NEW QUESTION 238

- (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 241

- (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 244

- (Exam Topic 3)

Which of the following BEST indicates how well a web infrastructure protects critical information from an attacker?

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

Answer: D

NEW QUESTION 245

- (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 250

- (Exam Topic 3)

Which of the following is the BEST key control indicator (KCI) for risk related to IT infrastructure failure?

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

Answer: B

NEW QUESTION 255

- (Exam Topic 3)

Which of the following scenarios represents a threat?

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

Answer: D

NEW QUESTION 260

- (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 262

- (Exam Topic 3)

When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs?

- A. Risk management
- B. Change management
- C. Problem management
- D. Quality management

Answer: B

NEW QUESTION 265

- (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 269

- (Exam Topic 3)

Which of the following is the MOST important objective of an enterprise risk management (ERM) program?

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

Answer: B

NEW QUESTION 272

- (Exam Topic 3)

Which of the following provides the MOST useful information when determining if a specific control should be implemented?

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

Answer: B

NEW QUESTION 277

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 281

- (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 286

- (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 290

- (Exam Topic 3)

The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

- A. obtain the support of executive management.
- B. map the business processes to supporting IT and other corporate resources.
- C. identify critical business processes and the degree of reliance on support services.
- D. document the disaster recovery process.

Answer: C

NEW QUESTION 292

- (Exam Topic 3)

A risk practitioner is preparing a report to communicate changes in the risk and control environment. The BEST way to engage stakeholder attention is to:

- A. include detailed deviations from industry benchmarks,
- B. include a summary linking information to stakeholder needs,
- C. include a roadmap to achieve operational excellence,
- D. publish the report on-demand for stakeholders.

Answer: B

NEW QUESTION 294

- (Exam Topic 3)

Which of the following provides the MOST useful information to determine risk exposure following control implementations?

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

Answer: C

NEW QUESTION 298

- (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 299

- (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 303

- (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 304

- (Exam Topic 3)

The risk associated with an asset after controls are applied can be expressed as:

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

Answer: C

NEW QUESTION 305

- (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 309

- (Exam Topic 3)

Which of the following is the BEST way to mitigate the risk to IT infrastructure availability?

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

Answer: D

NEW QUESTION 313

- (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 316

- (Exam Topic 3)

Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

- A. Financial risk is given a higher priority.
- B. Risk with strategic impact is included.
- C. Security strategy is given a higher priority.
- D. Risk identified by industry benchmarking is included.

Answer: B

NEW QUESTION 319

- (Exam Topic 3)

A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?

- A. Third-party software is used for data analytics.
- B. Data usage exceeds individual consent.
- C. Revenue generated is not disclosed to customers.
- D. Use of a data analytics system is not disclosed to customers.

Answer: B

NEW QUESTION 322

- (Exam Topic 3)

An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?

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

Answer: B

NEW QUESTION 325

- (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 327

- (Exam Topic 3)

Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

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

Answer: D

NEW QUESTION 330

- (Exam Topic 3)

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

- A. Implement segregation of duties.
- B. Enforce an internal data access policy.
- C. Enforce the use of digital signatures.
- D. Apply single sign-on for access control.

Answer: B

NEW QUESTION 334

- (Exam Topic 3)

What are the MOST essential attributes of an effective Key control indicator (KCI)?

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

Answer: B

NEW QUESTION 337

- (Exam Topic 3)

Which of the following data would be used when performing a business impact analysis (BIA)?

- A. Cost-benefit analysis of running the current business

- B. Cost of regulatory compliance
- C. Projected impact of current business on future business
- D. Expected costs for recovering the business

Answer: D

NEW QUESTION 338

- (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 342

- (Exam Topic 3)

The PRIMARY objective of a risk identification process is to:

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

Answer: B

NEW QUESTION 346

- (Exam Topic 3)

What is the PRIMARY benefit of risk monitoring?

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

Answer: C

NEW QUESTION 349

- (Exam Topic 3)

In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

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

Answer: B

NEW QUESTION 352

- (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 357

- (Exam Topic 3)

Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

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

Answer: C

NEW QUESTION 360

- (Exam Topic 3)

An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

- A. Sufficient resources are not assigned to IT development projects.
- B. Customer support help desk staff does not have adequate training.
- C. Email infrastructure does not have proper rollback plans.
- D. The corporate email system does not identify and store phishing emails.

Answer: A

NEW QUESTION 365

- (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 368

- (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 370

- (Exam Topic 3)

When formulating a social media policy to address information leakage, which of the following is the MOST important concern to address?

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

Answer: A

NEW QUESTION 371

- (Exam Topic 3)

Which of the following should be the PRIMARY focus of an IT risk awareness program?

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

Answer: B

NEW QUESTION 372

- (Exam Topic 3)

Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

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

Answer: B

NEW QUESTION 375

- (Exam Topic 3)

To communicate the risk associated with IT in business terms, which of the following MUST be defined?

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

Answer: C

NEW QUESTION 380

- (Exam Topic 3)

The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

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

Answer: D

NEW QUESTION 383

- (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 384

- (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 386

- (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 391

- (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 393

- (Exam Topic 3)

Which of the following is the GREATEST advantage of implementing a risk management program?

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

Answer: A

NEW QUESTION 396

- (Exam Topic 3)

Which of the following BEST enables an organization to determine whether external emerging risk factors will impact the organization's risk profile?

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

Answer: D

NEW QUESTION 400

- (Exam Topic 3)

Which of the following is the BEST way to quantify the likelihood of risk materialization?

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

Answer: D

NEW QUESTION 401

- (Exam Topic 3)

An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:

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

Answer: D

NEW QUESTION 406

- (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 410

- (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 411

- (Exam Topic 3)

Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

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

Answer: B

NEW QUESTION 415

- (Exam Topic 3)

Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?

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

Answer: A

NEW QUESTION 420

- (Exam Topic 3)

Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

- A. Percentage of unpatched IT assets
- B. Percentage of IT assets without ownership
- C. The number of IT assets securely disposed during the past year

D. The number of IT assets procured during the previous month

Answer: B

NEW QUESTION 421

- (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 426

- (Exam Topic 4)

Which of the following situations presents the GREATEST challenge to creating a comprehensive IT risk profile of an organization?

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

Answer: D

NEW QUESTION 429

- (Exam Topic 4)

Which of the following is the MOST important characteristic of a key risk indicator (KRI) to enable decision-making?

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

Answer: D

NEW QUESTION 433

- (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 434

- (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 438

- (Exam Topic 4)

Which of the following is MOST helpful in defining an early-warning threshold associated with insufficient network bandwidth?"

- A. Average bandwidth usage
- B. Peak bandwidth usage
- C. Total bandwidth usage
- D. Bandwidth used during business hours

Answer: A

NEW QUESTION 443

- (Exam Topic 4)

An information security audit identified a risk resulting from the failure of an automated control Who is responsible for ensuring the risk register is updated

accordingly?

- A. The risk practitioner
- B. The risk owner
- C. The control owner
- D. The audit manager

Answer: A

NEW QUESTION 447

- (Exam Topic 4)

Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?

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

Answer: C

NEW QUESTION 452

- (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 457

- (Exam Topic 4)

Which of the following is the BEST way to ensure adequate resources will be allocated to manage identified risk?

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

Answer: D

NEW QUESTION 459

- (Exam Topic 4)

An organization has agreed to a 99% availability for its online services and will not accept availability that falls below 98.5%. This is an example of:

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

Answer: C

NEW QUESTION 463

- (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 466

- (Exam Topic 4)

Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board?"

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

Answer: C

NEW QUESTION 470

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 473

- (Exam Topic 4)

Which of the following has the GREATEST influence on an organization's risk appetite?

- A. Threats and vulnerabilities
- B. Internal and external risk factors
- C. Business objectives and strategies
- D. Management culture and behavior

Answer: D

NEW QUESTION 478

- (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 481

- (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 483

- (Exam Topic 4)

Which of the following activities BEST facilitates effective risk management throughout the organization?

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

Answer: B

NEW QUESTION 488

- (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 appetite

Answer: B

NEW QUESTION 491

- (Exam Topic 4)

Which of the following provides the MOST comprehensive information when developing a risk profile for a system?

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

Answer: B

NEW QUESTION 493

- (Exam Topic 4)

Business management is seeking assurance from the CIO that IT has a plan in place for early identification of potential issues that could impact the delivery of a new application. Which of the following is the BEST way to increase the chances of a successful delivery'?

- A. Implement a release and deployment plan
- B. Conduct comprehensive regression testing.
- C. Develop enterprise-wide key risk indicators (KRIs)
- D. Include business management on a weekly risk and issues report

Answer: D

NEW QUESTION 497

- (Exam Topic 4)

When implementing an IT risk management program, which of the following is the BEST time to evaluate current control effectiveness?

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

Answer: B

NEW QUESTION 498

- (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 500

- (Exam Topic 4)

During an acquisition, which of the following would provide the MOST useful input to the parent company's risk practitioner when developing risk scenarios for the post-acquisition phase?

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

Answer: C

NEW QUESTION 504

- (Exam Topic 4)

An incentive program is MOST likely implemented to manage the risk associated with loss of which organizational asset?

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

Answer: A

NEW QUESTION 509

- (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 513

- (Exam Topic 4)

An organization's chief information officer (CIO) has proposed investing in a new, untested technology to take advantage of being first to market. Senior management has concerns about the success of the project and has set a limit for expenditures before final approval. This conditional approval indicates the organization's risk:

- A. capacity.
- B. appetite.

- C. management capability.
- D. treatment strategy.

Answer: B

NEW QUESTION 515

- (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 517

- (Exam Topic 4)

An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate this risk?

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

Answer: C

NEW QUESTION 520

- (Exam Topic 4)

When preparing a risk status report for periodic review by senior management, it is MOST important to ensure the report includes

- A. risk exposure in business terms
- B. a detailed view of individual risk exposures
- C. a summary of incidents that have impacted the organization.
- D. recommendations by an independent risk assessor.

Answer: A

NEW QUESTION 524

- (Exam Topic 4)

Which of the following would MOST likely require a risk practitioner to update the risk register?

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

Answer: C

NEW QUESTION 529

- (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 534

- (Exam Topic 4)

The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

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

Answer: C

NEW QUESTION 535

- (Exam Topic 4)

Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

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

Answer: C

NEW QUESTION 540

- (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 544

- (Exam Topic 4)

An organization wants to launch a campaign to advertise a new product Using data analytics, the campaign can be targeted to reach potential customers. Which of the following should be of **GREATEST** concern to the risk practitioner?

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

Answer: D

NEW QUESTION 547

- (Exam Topic 4)

When developing risk scenario using a list of generic scenarios based on industry best practices, it is **MOST** imported to:

- A. Assess generic risk scenarios with business users.
- B. Validate the generic risk scenarios for relevance.
- C. Select the maximum possible risk scenarios from the list.
- D. Identify common threats causing generic risk scenarios

Answer: B

NEW QUESTION 548

- (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 550

- (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 551

- (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 554

- (Exam Topic 4)

An organization control environment is MOST effective when:

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

Answer: B

NEW QUESTION 557

- (Exam Topic 4)

Which of the following is the BEST recommendation to address recent IT risk trends that indicate social engineering attempts are increasing in the organization?

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

Answer: A

NEW QUESTION 558

- (Exam Topic 4)

Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

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

Answer: C

NEW QUESTION 559

- (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 563

- (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 568

- (Exam Topic 4)

Who is MOST appropriate to be assigned ownership of a control

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

Answer: D

NEW QUESTION 573

- (Exam Topic 4)

Which of the following is the MOST important consideration when communicating the risk associated with technology end-of-life to business owners?

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

Answer: A

NEW QUESTION 574

- (Exam Topic 4)

Which of the following is MOST helpful in identifying loss magnitude during risk analysis of a new system?

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

Answer: C

NEW QUESTION 578

- (Exam Topic 4)

A control process has been implemented in response to a new regulatory requirement, but has significantly reduced productivity. Which of the following is the BEST way to resolve this concern?

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

Answer: C

NEW QUESTION 580

- (Exam Topic 4)

Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

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

Answer: B

NEW QUESTION 582

- (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 587

- (Exam Topic 4)

Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

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

Answer: A

NEW QUESTION 592

- (Exam Topic 4)

An organization is considering the adoption of an aggressive business strategy to achieve desired growth. From a risk management perspective, what should the risk practitioner do NEXT?

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

Answer: A

NEW QUESTION 597

- (Exam Topic 4)

The MAJOR reason to classify information assets is

- A. maintain a current inventory and catalog of information assets
- B. determine their sensitivity and critical
- C. establish recovery time objectives (RTOs)
- D. categorize data into groups

Answer: C

NEW QUESTION 602

- (Exam Topic 4)

Which of the following BEST helps to identify significant events that could impact an organization?

- A. Control analysis
- B. Vulnerability analysis
- C. Scenario analysis
- D. Heat map analysis

Answer: C

NEW QUESTION 603

- (Exam Topic 4)

Which of the following is the PRIMARY reason to perform periodic vendor risk assessments?

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

Answer: B

NEW QUESTION 606

- (Exam Topic 4)

In order to efficiently execute a risk response action plan, it is MOST important for the emergency response team members to understand:

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

Answer: D

NEW QUESTION 610

- (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 615

- (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 619

- (Exam Topic 4)

Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

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

Answer: A

NEW QUESTION 624

- (Exam Topic 4)

Which of the following proposed benefits is MOST likely to influence senior management approval to reallocate budget for a new security initiative?

- A. Reduction in the number of incidents
- B. Reduction in inherent risk
- C. Reduction in residual risk

D. Reduction in the number of known vulnerabilities

Answer: B

NEW QUESTION 626

- (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 627

- (Exam Topic 4)

Which of the following is the PRIMARY objective of establishing an organization's risk tolerance and appetite?

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

Answer: B

NEW QUESTION 628

- (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 633

- (Exam Topic 4)

Which of the following is the BEST course of action when an organization wants to reduce likelihood in order to reduce a risk level?

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

Answer: B

NEW QUESTION 636

- (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 641

- (Exam Topic 4)

Which of the following is MOST important information to review when developing plans for using emerging technologies?

- A. Existing IT environment
- B. IT strategic plan
- C. Risk register
- D. Organizational strategic plan

Answer: D

NEW QUESTION 645

- (Exam Topic 4)

Which of the following is a risk practitioner's BEST recommendation upon learning that an employee inadvertently disclosed sensitive data to a vendor?

- A. Enroll the employee in additional security training.

- B. Invoke the incident response plan.
- C. Conduct an internal audit.
- D. Instruct the vendor to delete the data.

Answer: B

NEW QUESTION 647

- (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 651

- (Exam Topic 4)

Before assigning sensitivity levels to information it is MOST important to:

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

Answer: B

NEW QUESTION 652

- (Exam Topic 4)

Which of the following is MOST useful for measuring the existing risk management process against a desired state?

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

Answer: C

NEW QUESTION 657

- (Exam Topic 4)

Which of the following is MOST important to include when reporting the effectiveness of risk management to senior management?

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

Answer: C

NEW QUESTION 661

- (Exam Topic 4)

Which of the following is MOST important for senior management to review during an acquisition?

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

Answer: A

NEW QUESTION 663

- (Exam Topic 4)

Which of the following is MOST important to update when an organization's risk appetite changes?

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

Answer: A

NEW QUESTION 664

- (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 665

- (Exam Topic 4)

Which key performance efficiency (KPI) BEST measures the effectiveness of an organization's disaster recovery program?

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

Answer: D

NEW QUESTION 668

- (Exam Topic 4)

Which of the following would be the GREATEST concern for an IT risk practitioner when an employee.....

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

Answer: B

NEW QUESTION 670

- (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 671

- (Exam Topic 4)

Of the following, who is responsible for approval when a change in an application system is ready for release to production?

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

Answer: C

NEW QUESTION 676

- (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 677

- (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 680

- (Exam Topic 4)

Which of the following is the MOST useful information for a risk practitioner when planning response activities after risk identification?

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

Answer: B

NEW QUESTION 685

- (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 686

- (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 689

- (Exam Topic 4)

After the implementation of Internet of Things (IoT) devices, new risk scenarios were identified. What is the PRIMARY reason to report this information to risk owners?

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

Answer: D

NEW QUESTION 690

- (Exam Topic 4)

When evaluating a number of potential controls for treating risk, it is MOST important to consider:

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

Answer: C

NEW QUESTION 691

- (Exam Topic 4)

Which organization is implementing a project to automate the purchasing process, including the modification of approval controls. Which of the following tasks is the responsibility of the risk practitioner*?

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

Answer: B

NEW QUESTION 692

- (Exam Topic 4)

An organization is implementing robotic process automation (RPA) to streamline business processes. Given that implementation of this technology is expected to impact existing controls, which of the following is the risk practitioner's BEST course of action?

- A. Reassess whether mitigating controls address the known risk in the processes.
- B. Update processes to address the new technology.
- C. Update the data governance policy to address the new technology.
- D. Perform a gap analysis of the impacted processes.

Answer: A

NEW QUESTION 693

- (Exam Topic 4)

Which of the following is MOST important to determine as a result of a risk assessment?

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

Answer: D

NEW QUESTION 698

- (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 702

- (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 706

- (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 709

- (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 711

- (Exam Topic 4)

A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

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

Answer: B

NEW QUESTION 715

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 720

- (Exam Topic 4)

During a risk assessment, a risk practitioner learns that an IT risk factor is adequately mitigated by compensating controls in an associated business process. Which of the following would enable the MOST effective management of the residual risk?

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

Answer: A

NEW QUESTION 724

- (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 downtime 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 725

- (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 728

- (Exam Topic 4)

Which of the following is a risk practitioner's BEST course of action after identifying risk scenarios related to noncompliance with new industry regulations?

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

Answer: D

NEW QUESTION 729

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 733

- (Exam Topic 3)

Which of the following trends would cause the GREATEST concern regarding the effectiveness of an organization's user access control processes? An increase in the:

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

Answer: D

NEW QUESTION 737

- (Exam Topic 3)

What information is MOST helpful to asset owners when classifying organizational assets for risk assessment?

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

Answer: A

NEW QUESTION 738

- (Exam Topic 3)

Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

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

Answer: A

NEW QUESTION 740

- (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 745

- (Exam Topic 3)

A risk practitioner has just learned about new malware that has severely impacted industry peers worldwide data loss?

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

Answer: B

NEW QUESTION 749

- (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 750

- (Exam Topic 3)

Which of the following would MOST likely cause a risk practitioner to change the likelihood rating in the risk register?

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

Answer: C

NEW QUESTION 753

- (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 754

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 756

- (Exam Topic 3)

Which of the following would BEST mitigate the risk associated with reputational damage from inappropriate use of social media sites by employees?

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

Answer: D

NEW QUESTION 761

- (Exam Topic 3)

Which of the following describes the relationship between Key risk indicators (KRIs) and key control indicators (KCIS)?

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

Answer: D

NEW QUESTION 763

- (Exam Topic 3)

When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

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

Answer: B

NEW QUESTION 764

- (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 768

- (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 771

- (Exam Topic 3)

Which of the following is MOST important to communicate to senior management during the initial implementation of a risk management program?

- A. Regulatory compliance
- B. Risk ownership
- C. Best practices
- D. Desired risk level

Answer: D

NEW QUESTION 774

- (Exam Topic 3)

A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

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

Answer: D

NEW QUESTION 775

- (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 780

- (Exam Topic 3)

Which of the following BEST indicates that additional or improved controls are needed in the environment?

- A. Management has decreased organisational risk appetite
- B. The risk register and portfolio do not include all risk scenarios
- C. Emerging risk scenarios have been identified
- D. Risk events and losses exceed risk tolerance

Answer: D

NEW QUESTION 784

- (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 787

- (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 789

- (Exam Topic 3)

Which of the following BEST informs decision-makers about the value of a notice and consent control for the collection of personal information?

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

Answer: D

NEW QUESTION 794

- (Exam Topic 3)

An organization planning to transfer and store its customer data with an offshore cloud service provider should be PRIMARILY concerned with:

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

Answer: B

NEW QUESTION 799

- (Exam Topic 3)

Which of the following practices BEST mitigates risk related to enterprise-wide ethical decision making in a multi-national organization?

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

Answer: A

NEW QUESTION 800

- (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 802

- (Exam Topic 3)

Prudent business practice requires that risk appetite not exceed:

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

Answer: C

NEW QUESTION 805

- (Exam Topic 3)

Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

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

Answer: A

NEW QUESTION 809

- (Exam Topic 3)

Which of the following is the STRONGEST indication an organization has ethics management issues?

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

Answer: A

NEW QUESTION 812

- (Exam Topic 3)

Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 813

- (Exam Topic 3)

After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?

- A. Obtain industry benchmarks related to the specific risk.
- B. Provide justification for the lower risk rating.
- C. Notify the business at the next risk briefing.
- D. Reopen the risk issue and complete a full assessment.

Answer: B

NEW QUESTION 817

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 822

- (Exam Topic 3)

Which of the following is the BEST course of action to help reduce the probability of an incident recurring?

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

Answer: B

NEW QUESTION 827

- (Exam Topic 3)

Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

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

Answer: C

NEW QUESTION 831

- (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 833

- (Exam Topic 3)

Which of the following poses the GREATEST risk to an organization's operations during a major IT transformation?

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

Answer: D

NEW QUESTION 835

- (Exam Topic 3)

Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

- A. Improved senior management communication

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

Answer: B

NEW QUESTION 839

- (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 840

- (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 843

- (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 846

- (Exam Topic 3)

A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

- A. Monitor the databases for abnormal activity
- B. Approve exception to allow the software to continue operating
- C. Require the software vendor to remediate the vulnerabilities
- D. Accept the risk and let the vendor run the software as is

Answer: C

NEW QUESTION 851

- (Exam Topic 3)

Which of the following is the PRIMARY reason to adopt key control indicators (KCIs) in the risk monitoring and reporting process?

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

Answer: D

NEW QUESTION 853

- (Exam Topic 3)

A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:

- A. management.
- B. tolerance.
- C. culture.
- D. analysis.

Answer: C

NEW QUESTION 858

- (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 862

- (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 866

- (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 868

- (Exam Topic 3)

Which of the following is MOST helpful to mitigate the risk associated with an application under development not meeting business objectives?

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

Answer: D

NEW QUESTION 869

- (Exam Topic 3)

A risk practitioner has become aware of production data being used in a test environment. Which of the following should be the practitioner's PRIMARY concern?

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

Answer: A

NEW QUESTION 871

- (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 876

- (Exam Topic 3)

Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

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

Answer: C

NEW QUESTION 881

- (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 885

- (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 889

- (Exam Topic 3)

Which of the following would be a risk practitioner's BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

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

Answer: B

NEW QUESTION 894

- (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 896

.....

Relate Links

100% Pass Your CRISC Exam with ExamBible Prep Materials

<https://www.exambible.com/CRISC-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>