



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

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

**Answer: B**

#### NEW QUESTION 6

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 7

- (Exam Topic 4)

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

- A. IT security managers
- B. IT control owners
- C. IT auditors

D. IT risk owners

**Answer:** D

#### NEW QUESTION 8

- (Exam Topic 4)

An organization'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 would provide the MOST useful input when evaluating the appropriateness of risk responses?

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

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 4)

Which of the following is 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 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 14

- (Exam Topic 4)

A poster has been displayed in a data center that reads. "Anyone caught taking photographs in the data center may be subject to disciplinary action." Which of the following control types has been implemented?

- A. Corrective
- B. Detective
- C. Deterrent
- D. Preventative

**Answer:** A

#### NEW QUESTION 16

- (Exam Topic 4)

The MOST important measure of the effectiveness of risk management in project implementation is the percentage of projects:

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

**Answer:** A

#### NEW QUESTION 17

- (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 19

- (Exam Topic 4)

Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

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

**Answer:** D

#### NEW QUESTION 20

- (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 22

- (Exam Topic 4)

Which of the following roles should be assigned accountability for monitoring risk levels?

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

**Answer:** C

#### NEW QUESTION 27

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 31

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 34

- (Exam Topic 4)

Which of the following should be the FIRST consideration when establishing a new risk governance program?

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

**Answer: B**

#### NEW QUESTION 36

- (Exam Topic 4)

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

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

**Answer: D**

#### NEW QUESTION 41

- (Exam Topic 4)

A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

- A. risk score
- B. risk impact
- C. risk response
- D. risk likelihood.

**Answer: B**

#### NEW QUESTION 45

- (Exam Topic 4)

A root cause analysis indicates a major service disruption due to a lack of competency of newly hired IT system administrators. Who should be accountable for resolving the situation?

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

**Answer: C**

#### NEW QUESTION 47

- (Exam Topic 4)

Which of the following would provide the BEST evidence of an effective internal control environment/?

- A. Risk assessment results
- B. Adherence to governing policies
- C. Regular stakeholder briefings
- D. Independent audit results

**Answer: D**

#### NEW QUESTION 51

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 52

- (Exam Topic 4)

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

- A. review alignment with the organization's 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 53**

- (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 the next assessment

**Answer:** A

**NEW QUESTION 55**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 60**

- (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 62**

- (Exam Topic 4)

An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis. Which of the following is the MOST important control to ensure the privacy of customer information?

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

**Answer:** C

**NEW QUESTION 66**

- (Exam Topic 4)

What is senior management's role in the RACI model when tasked with reviewing monthly status reports provided by risk owners?

- A. Accountable
- B. Informed
- C. Responsible
- D. Consulted

**Answer:** B

**NEW QUESTION 69**

- (Exam Topic 4)

Which of the following is the MOST effective way to help ensure accountability for managing risk?

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

**Answer:** A

**NEW QUESTION 71**

- (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 72

- (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 77

- (Exam Topic 4)

Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

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

**Answer:** A

#### NEW QUESTION 81

- (Exam Topic 4)

Which of the following is the PRIMARY purpose of creating and documenting control procedures?

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

**Answer:** D

#### NEW QUESTION 84

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 87

- (Exam Topic 3)

Which of The following should be of GREATEST concern for an organization considering the adoption of a bring your own device (BYOD) initiative?

- A. Device corruption
- B. Data loss
- C. Malicious users
- D. User support

**Answer:** B

#### NEW QUESTION 91

- (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 92



- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 95

- (Exam Topic 4)

Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?

- A. Fiscal management practices
- B. Business maturity
- C. Budget for implementing security
- D. Management culture

**Answer: D**

#### NEW QUESTION 97

- (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 101

- (Exam Topic 3)

Which of the following is the MOST effective control to maintain the integrity of system configuration files?

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

**Answer: D**

#### NEW QUESTION 104

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 105

- (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 106

- (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 108

- (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 112

- (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 115

- (Exam Topic 3)

A financial institution has identified high risk of fraud in several business applications. Which of the following controls will BEST help reduce the risk of fraudulent internal transactions?

- A. Periodic user privileges review
- B. Log monitoring
- C. Periodic internal audits
- D. Segregation of duties

**Answer:** A

#### NEW QUESTION 120

- (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 123

- (Exam Topic 3)

Which of the following is MOST important to include in a risk assessment of an emerging technology?

- A. Risk response plans
- B. Risk and control ownership
- C. Key controls
- D. Impact and likelihood ratings

**Answer:** D

#### NEW QUESTION 125

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 129

- (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 131**

- (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 136**

- (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 141**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 145**

- (Exam Topic 3)

Which of the following should be the FIRST consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected?

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

**Answer:** A

**NEW QUESTION 148**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 149**

- (Exam Topic 3)

A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

- A. better understands the system architecture.
- B. is more objective than risk management.
- C. can balance technical and business risk.
- D. can make better-informed business decisions.

**Answer:** D

**NEW QUESTION 150**

- (Exam Topic 3)

An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

- A. Potential increase in regulatory scrutiny

- B. Potential system downtime
- C. Potential theft of personal information
- D. Potential legal risk

**Answer:** C

#### NEW QUESTION 151

- (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 152

- (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 153

- (Exam Topic 3)

Which of the following should be an element of the risk appetite of an organization?

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

**Answer:** B

#### NEW QUESTION 156

- (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 158

- (Exam Topic 3)

While evaluating control costs, management discovers that the annual cost exceeds the annual loss expectancy (ALE) of the risk. This indicates the:

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

**Answer:** B

#### NEW QUESTION 159

- (Exam Topic 3)

Which of the following should be the GREATEST concern for an organization that uses open source software applications?

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

**Answer:** A

#### NEW QUESTION 160

- (Exam Topic 3)

An IT department originally planned to outsource the hosting of its data center at an overseas location to reduce operational expenses. After a risk assessment,

the department has decided to keep the data center in-house. How should the risk treatment response be reflected in the risk register?

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

**Answer:** A

#### NEW QUESTION 161

- (Exam Topic 3)

Which of the following is the PRIMARY risk management responsibility of the second line of defense?

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

**Answer:** A

#### NEW QUESTION 166

- (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 167

- (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 170

- (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 174

- (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 178

- (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 180

- (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 182

- (Exam Topic 3)

Which of the following should be determined FIRST when a new security vulnerability is made public?

- A. Whether the affected technology is used within the organization
- B. Whether the affected technology is Internet-facing
- C. What mitigating controls are currently in place
- D. How pervasive the vulnerability is within the organization

**Answer: A**

#### NEW QUESTION 186

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 187

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 191

- (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 193

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 195

- (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 198**

- (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 200**

- (Exam Topic 3)

Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

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

**Answer:** D

**NEW QUESTION 204**

- (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 209**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 210**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 214**

- (Exam Topic 3)

The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:

- A. inconsistencies between security policies and procedures
- B. possible noncompliant activities that lead to data disclosure
- C. leading or lagging key risk indicators (KRIs)
- D. unknown threats to undermine existing access controls

**Answer:** B

**NEW QUESTION 217**

- (Exam Topic 3)

A risk practitioner identifies a database application that has been developed and implemented by the business independently of IT. Which of the following is the BEST course of action?



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

**Answer:** B

#### NEW QUESTION 221

- (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 222

- (Exam Topic 3)

Which of the following will BEST support management reporting on risk?

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

**Answer:** C

#### NEW QUESTION 223

- (Exam Topic 3)

Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

- A. Align business objectives with risk appetite.
- B. Enable risk-based decision making.
- C. Design and implement risk response action plans.
- D. Update risk responses in the risk register

**Answer:** B

#### NEW QUESTION 225

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 226

- (Exam Topic 3)

Vulnerabilities have been detected on an organization's systems. Applications installed on these systems will not operate if the underlying servers are updated. Which of the following is the risk practitioner's BEST course of action?

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

**Answer:** D

#### NEW QUESTION 230

- (Exam Topic 3)

Which of The following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?

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

**Answer:** C

#### NEW QUESTION 231

- (Exam Topic 3)

Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

- A. Obtain objective assessment of the control environment.
- B. Ensure the risk profile is defined and communicated.
- C. Validate the threat management process.
- D. Obtain an objective view of process gaps and systemic errors.

**Answer:** A

#### NEW QUESTION 234

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 236

- (Exam Topic 3)

Which of the following is the BEST Key control indicator KCO to monitor the effectiveness of patch management?

- A. Percentage of legacy servers out of support
- B. Percentage of servers receiving automata patches
- C. Number of unremediated vulnerabilities
- D. Number of intrusion attempts

**Answer:** D

#### NEW QUESTION 239

- (Exam Topic 3)

When of the following 15 MOST important when developing a business case for a proposed security investment?

- A. identification of control requirements
- B. Alignment to business objectives
- C. Consideration of new business strategies
- D. inclusion of strategy for regulatory compliance

**Answer:** B

#### NEW QUESTION 240

- (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 241

- (Exam Topic 3)

While reviewing the risk register, a risk practitioner notices that different business units have significant variances in inherent risk for the same risk scenario. Which of the following is the BEST course of action?

- A. Update the risk register with the average of residual risk for both business units.
- B. Review the assumptions of both risk scenarios to determine whether the variance is reasonable.
- C. Update the risk register to ensure both risk scenarios have the highest residual risk.
- D. Request that both business units conduct another review of the risk.

**Answer:** B

#### NEW QUESTION 242

- (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 244

- (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 248

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 251

- (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 252

- (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 256

- (Exam Topic 3)

Which of the following practices MOST effectively safeguards the processing of personal data?

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

**Answer:** B

#### NEW QUESTION 260

- (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 265

- (Exam Topic 3)

Which of the following is necessary to enable an IT risk register to be consolidated with the rest of the organization's risk register?

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

**Answer:**

A

#### NEW QUESTION 266

- (Exam Topic 3)

Which of the following is the MOST important consideration for protecting data assets in a Business application system?

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

**Answer:** A

#### NEW QUESTION 271

- (Exam Topic 3)

Legal and regulatory risk associated with business conducted over the Internet is driven by:

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

**Answer:** C

#### NEW QUESTION 272

- (Exam Topic 3)

Which of the following is the BEST evidence of an effective risk treatment plan?

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

**Answer:** B

#### NEW QUESTION 275

- (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 278

- (Exam Topic 3)

Which of the following is MOST important to the integrity of a security log?

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

**Answer:** B

#### NEW QUESTION 279

- (Exam Topic 3)

Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

- A. Key risk indicators (KRIs)
- B. Risk scenarios
- C. Business impact analysis (BIA)
- D. Threat analysis

**Answer:** B

#### NEW QUESTION 282

- (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 286

- (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 289

- (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 292

- (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 296

- (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 298

- (Exam Topic 3)

A risk practitioner is developing a set of bottom-up IT risk scenarios. The MOST important time to involve business stakeholders is when:

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

**Answer:** C

#### NEW QUESTION 303

- (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 307

- (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 309

- (Exam Topic 3)

Which of the following is MOST important to the successful development of IT risk scenarios?

- A. Cost-benefit analysis
- B. Internal and external audit reports
- C. Threat and vulnerability analysis
- D. Control effectiveness assessment

**Answer:** C

#### NEW QUESTION 310

- (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 312

- (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 317

- (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 322

- (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 327

- (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 329

- (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 333

- (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 334

- (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 336

- (Exam Topic 3)

In which of the following system development life cycle (SDLC) phases should controls be incorporated into system specifications?

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

**Answer:** C

#### NEW QUESTION 341

- (Exam Topic 3)

Which of the following would be MOST helpful when communicating roles associated with the IT risk management process?

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

**Answer:** A

#### NEW QUESTION 342

- (Exam Topic 3)

Who is BEST suited to determine whether a new control properly mitigates data loss risk within a system?

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

**Answer:** B

#### NEW QUESTION 343

- (Exam Topic 3)

Which of the following is the MOST effective control to address the risk associated with compromising data privacy within the cloud?

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

**Answer:** D

#### NEW QUESTION 344



- (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 347

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 349

- (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 354

- (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 355

- (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 356

- (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 358

- (Exam Topic 4)

Recovery the objectives (RTOs) should be based on

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

**Answer:** C

#### NEW QUESTION 359

- (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 362

- (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 363

- (Exam Topic 4)

Which of the following is MOST helpful to understand the consequences of an IT risk event?

- A. Fault tree analysis
- B. Historical trend analysis
- C. Root cause analysis
- D. Business impact analysis (BIA)

**Answer:** B

#### NEW QUESTION 367

- (Exam Topic 4)

Reviewing which of the following BEST helps an organization gain insight into its overall risk profile"

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

**Answer:** B

#### NEW QUESTION 372

- (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 376

- (Exam Topic 4)

Which risk response strategy could management apply to both positive and negative risk that has been identified?

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

**Answer:** B

#### NEW QUESTION 381

- (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 383

- (Exam Topic 4)

Who should be responsible (of evaluating the residual risk after a compensating control has been

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

**Answer: D**

#### NEW QUESTION 386

- (Exam Topic 4)

An organization is analyzing the risk of shadow IT usage. Which of the following is the MOST important input into the assessment?

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

**Answer: A**

#### NEW QUESTION 390

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 394

- (Exam Topic 4)

Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

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

**Answer: D**

#### NEW QUESTION 399

- (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 402

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 403

- (Exam Topic 4)

Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

- A. Verifying that project objectives are met
- B. Identifying project cost overruns
- C. Leveraging an independent review team

D. Reviewing the project initiation risk matrix

**Answer:** A

#### NEW QUESTION 406

- (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 407

- (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 412

- (Exam Topic 4)

The MAIN reason for prioritizing IT risk responses is to enable an organization to:

- A. determine the risk appetite.
- B. determine the budget.
- C. define key performance indicators (KPIs).
- D. optimize resource utilization.

**Answer:** C

#### NEW QUESTION 414

- (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 415

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 419

- (Exam Topic 4)

The BEST indicator of the risk appetite of an organization is the

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

**Answer:** B

#### NEW QUESTION 423

- (Exam Topic 4)

A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?

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

**Answer: D**

#### NEW QUESTION 424

- (Exam Topic 4)

An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

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

**Answer: D**

#### NEW QUESTION 426

- (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 428

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 431

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 432

- (Exam Topic 4)

An organization has operations in a location that regularly experiences severe weather events. Which of the following would BEST help to mitigate the risk to operations?

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

**Answer: D**

#### NEW QUESTION 433

- (Exam Topic 4)

Who is BEST suited to provide objective input when updating residual risk to reflect the results of control effectiveness?

- A. Control owner
- B. Risk owner
- C. Internal auditor
- D. Compliance manager

**Answer:** C

**NEW QUESTION 435**

- (Exam Topic 4)

When confirming whether implemented controls are operating effectively, which of the following is MOST important to review?

- A. Results of benchmarking studies
- B. Results of risk assessments
- C. Number of emergency change requests
- D. Maturity model

**Answer:** B

**NEW QUESTION 440**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 441**

- (Exam Topic 4)

A global organization has implemented an application that does not address all privacy requirements across multiple jurisdictions. Which of the following risk responses has the organization adopted with regard to privacy requirements?

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

**Answer:** A

**NEW QUESTION 443**

- (Exam Topic 4)

Which of the following is the BEST control to minimize the risk associated with scope creep in software development?

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

**Answer:** A

**NEW QUESTION 448**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 450**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 452**

- (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 455

- (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 460

- (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 testing the control
- D. The individual accountable for monitoring control effectiveness

**Answer:** D

#### NEW QUESTION 465

- (Exam Topic 4)

Which of the following is the BEST method to mitigate the risk of an unauthorized employee viewing confidential data in a database"

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

**Answer:** A

#### NEW QUESTION 466

- (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 467

- (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 472

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 476

- (Exam Topic 4)

Which of the following should be considered FIRST when creating a comprehensive IT risk register?



- A. Risk management budget
- B. Risk mitigation policies
- C. Risk appetite
- D. Risk analysis techniques

**Answer:** C

#### NEW QUESTION 478

- (Exam Topic 4)

An organization has experienced a cyber attack that exposed customer personally identifiable information (PII) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

- A. Security control owners based on control failures
- B. Cyber risk remediation plan owners
- C. Risk owners based on risk impact
- D. Enterprise risk management (ERM) team

**Answer:** C

#### NEW QUESTION 480

- (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 482

- (Exam Topic 4)

An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?

- A. Acquisition
- B. Implementation
- C. Initiation
- D. Operation and maintenance

**Answer:** C

#### NEW QUESTION 486

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 490

- (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 495

- (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 496

- (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 500

- (Exam Topic 4)

Which of the following is the PRIMARY objective of maintaining an information asset inventory?

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

**Answer: B**

#### NEW QUESTION 504

- (Exam Topic 4)

Which of the following is MOST helpful in providing an overview of an organization's risk management program?

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

**Answer: C**

#### NEW QUESTION 507

- (Exam Topic 4)

Which of the following will BEST help to ensure implementation of corrective action plans?

- A. Establishing employee awareness training
- B. Assigning accountability to risk owners
- C. Selling target dates to complete actions
- D. Contracting to third parties

**Answer: B**

#### NEW QUESTION 509

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 510

- (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 512

- (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 516

- (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 518

- (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 519

- (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 522

- (Exam Topic 4)

Which of the following is the result of a realized risk scenario?

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

**Answer:** D

#### NEW QUESTION 527

- (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 528

- (Exam Topic 4)

Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

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

**Answer:** B

#### NEW QUESTION 529

- (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 533

- (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 537

- (Exam Topic 4)

After an annual risk assessment is completed, which of the following would be MOST important to communicate to stakeholders?

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

**Answer: B**

#### NEW QUESTION 541

- (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 545

- (Exam Topic 4)

Which of the following is the MOST important step to ensure regulatory requirements are adequately addressed within an organization?

- A. Obtain necessary resources to address regulatory requirements
- B. Develop a policy framework that addresses regulatory requirements
- C. Perform a gap analysis against regulatory requirements.
- D. Employ IT solutions that meet regulatory requirements.

**Answer: B**

#### NEW QUESTION 550

- (Exam Topic 4)

Who is the BEST person to manage employee personal data?

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

**Answer: A**

#### NEW QUESTION 553

- (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 558

- (Exam Topic 4)

An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:

- A. a recognized industry control framework
- B. guidance provided by the external auditor

- C. the service provider's existing controls
- D. The organization's specific control requirements

**Answer:** D

#### NEW QUESTION 560

- (Exam Topic 4)

An IT risk threat analysis is BEST used to establish

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

**Answer:** A

#### NEW QUESTION 561

- (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 563

- (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 565

- (Exam Topic 4)

Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

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

**Answer:** A

#### NEW QUESTION 570

- (Exam Topic 4)

Which of the following is the GREATEST concern when establishing key risk indicators (KRIs)?

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

**Answer:** B

#### NEW QUESTION 575

- (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 578

- (Exam Topic 4)

Which of the following would be of GREATEST concern regarding an organization's asset management?

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

**Answer:** D

#### NEW QUESTION 580

- (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 583

- (Exam Topic 4)

The MAIN purpose of selecting a risk response is to.

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

**Answer:** C

#### NEW QUESTION 586

- (Exam Topic 4)

Which of the following should be the PRIMARY input to determine risk tolerance?

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

**Answer:** C

#### NEW QUESTION 590

- (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 591

- (Exam Topic 4)

A bank recently incorporated Blockchain technology with the potential to impact known risk within the organization. Which of the following is the risk practitioner's BEST course of action?

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

**Answer:** B

#### NEW QUESTION 595

- (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 600

- (Exam Topic 4)

The BEST key performance indicator (KPI) to measure the effectiveness of the security patching process is the percentage of patches installed:

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

**Answer:** B

#### NEW QUESTION 602

- (Exam Topic 4)

Which of the following should be the PRIMARY basis for prioritizing risk responses?

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

**Answer:** A

#### NEW QUESTION 605

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 608

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 613

- (Exam Topic 4)

Which of the following is MOST important when determining risk appetite?

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

**Answer:** C

#### NEW QUESTION 616

- (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 618

- (Exam Topic 4)

it was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern1?

- A. The underutilization of the replicated link
- B. The cost of recovering the data
- C. The lack of integrity of data
- D. The loss of data confidentiality

**Answer:**



C

#### NEW QUESTION 620

- (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 624

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 625

- (Exam Topic 3)

Which of the following should be implemented to BEST mitigate the risk associated with infrastructure updates?

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

**Answer:** C

#### NEW QUESTION 627

- (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 628

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 633

- (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 637

- (Exam Topic 3)

Which of the following BEST indicates that an organization has implemented IT performance requirements?

- A. Service level agreements (SLA)
- B. Vendor references

- C. Benchmarking data
- D. Accountability matrix

**Answer:** A

#### NEW QUESTION 639

- (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 644

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 645

- (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 649

- (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 654

- (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 657

- (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 658

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 661

- (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 663

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 666

- (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 670

- (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 674

- (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 675

- (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 676

- (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 677

- (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 678

- (Exam Topic 3)

Which of the following BEST assists in justifying an investment in automated controls?

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

**Answer:** A

#### NEW QUESTION 681

- (Exam Topic 3)

Of the following, who is accountable for ensuring the effectiveness of a control to mitigate risk?

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

**Answer:** A

#### NEW QUESTION 686

- (Exam Topic 3)

Which of the following is the FIRST step in risk assessment?

- A. Review risk governance
- B. Asset identification
- C. Identify risk factors
- D. Inherent risk identification

**Answer:** B

#### NEW QUESTION 689

- (Exam Topic 3)

Which of the following provides the BEST measurement of an organization's risk management maturity level?

- A. Level of residual risk
- B. The results of a gap analysis
- C. IT alignment to business objectives
- D. Key risk indicators (KRIs)

**Answer:** C

#### NEW QUESTION 690

- (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 694

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 696

- (Exam Topic 3)

What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

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

**Answer: A**

#### NEW QUESTION 701

- (Exam Topic 3)

The PRIMARY purpose of IT control status reporting is to:

- A. ensure compliance with IT governance strategy.
- B. assist internal audit in evaluating and initiating remediation efforts.
- C. benchmark IT controls with Industry standards.
- D. facilitate the comparison of the current and desired states.

**Answer: A**

#### NEW QUESTION 705

- (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 707

- (Exam Topic 3)

An organization automatically approves exceptions to security policies on a recurring basis. This practice is MOST likely the result of:

- A. a lack of mitigating actions for identified risk
- B. decreased threat levels
- C. ineffective service delivery
- D. ineffective IT governance

**Answer: D**

#### NEW QUESTION 710

- (Exam Topic 3)

The acceptance of control costs that exceed risk exposure MOST likely demonstrates:

- A. corporate culture alignment
- B. low risk tolerance
- C. high risk tolerance
- D. corporate culture misalignment.

**Answer: C**

#### NEW QUESTION 712

- (Exam Topic 3)

The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

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

**Answer:** A

#### NEW QUESTION 716

- (Exam Topic 3)

The MAIN purpose of reviewing a control after implementation is to validate that the control:

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

**Answer:** A

#### NEW QUESTION 717

- (Exam Topic 3)

Which of the following BEST mitigates the risk of sensitive personal data leakage from a software development environment?

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

**Answer:** C

#### NEW QUESTION 720

- (Exam Topic 3)

Which of the following BEST indicates the efficiency of a process for granting access privileges?

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

**Answer:** C

#### NEW QUESTION 724

- (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 727

- (Exam Topic 3)

Which of the following is the PRIMARY reason to adopt key control indicators (KCI) 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 729

- (Exam Topic 3)

Which of the following approaches would BEST help to identify relevant risk scenarios?

- A. Engage line management in risk assessment workshops.
- B. Escalate the situation to risk leadership.
- C. Engage internal audit for risk assessment workshops.
- D. Review system and process documentation.

**Answer:** A

#### NEW QUESTION 731

- (Exam Topic 3)

Which of the following should be done FIRST when information is no longer required to support business objectives?

- A. Archive the information to a backup database.
- B. Protect the information according to the classification policy.



- C. Assess the information against the retention policy.
- D. Securely and permanently erase the information

**Answer:** C

#### NEW QUESTION 736

- (Exam Topic 3)

Which of the following is the MOST common concern associated with outsourcing to a service provider?

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

**Answer:** C

#### NEW QUESTION 737

- (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 741

- (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 742

- (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 746

- (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 751

- (Exam Topic 3)

The GREATEST benefit of including low-probability, high-impact events in a risk assessment is the ability to:

- A. develop a comprehensive risk mitigation strategy
- B. develop understandable and realistic risk scenarios
- C. identify root causes for relevant events
- D. perform an aggregated cost-benefit analysis

**Answer:** D

#### NEW QUESTION 755

- (Exam Topic 3)

During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?

- A. Conduct a comprehensive review of access management processes.
- B. Declare a security incident and engage the incident response team.
- C. Conduct a comprehensive awareness session for system administrators.
- D. Evaluate system administrators' technical skills to identify if training is required.

**Answer:** A

#### NEW QUESTION 759

- (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 762

- (Exam Topic 3)

For a large software development project, risk assessments are MOST effective when performed:

- A. before system development begins.
- B. at system development.
- C. at each stage of the system development life cycle (SDLC).
- D. during the development of the business case.

**Answer:** C

#### NEW QUESTION 766

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 769

- (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 770

- (Exam Topic 3)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an antivirus program?

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

**Answer:** A

#### NEW QUESTION 771

- (Exam Topic 3)

Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:

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

**Answer:** B

#### NEW QUESTION 774

- (Exam Topic 3)

Which of the following **MUST** be updated to maintain an IT risk register?

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

**Answer: C**

#### NEW QUESTION 777

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 781

- (Exam Topic 3)

Which of the following is the **MOST** effective way to integrate risk and compliance management?

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

**Answer: A**

#### NEW QUESTION 785

- (Exam Topic 3)

Which of the following would **BEST** help to address the risk associated with malicious outsiders modifying application data?

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

**Answer: A**

#### NEW QUESTION 789

- (Exam Topic 3)

Accountability for a particular risk is **BEST** represented in a:

- A. risk register
- B. risk catalog
- C. risk scenario
- D. RACI matrix

**Answer: D**

#### NEW QUESTION 793

- (Exam Topic 3)

An IT risk practitioner has been asked to regularly report on the overall status and effectiveness of the IT risk management program. Which of the following is **MOST** useful for this purpose?

- A. Balanced scorecard
- B. Capability maturity level
- C. Internal audit plan
- D. Control self-assessment (CSA)

**Answer: A**

#### NEW QUESTION 797

- (Exam Topic 3)

While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The **BEST** course of action is to:

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

D. review the policies against current needs to determine adequacy.

**Answer:** D

#### NEW QUESTION 799

- (Exam Topic 3)

Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?

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

**Answer:** D

#### NEW QUESTION 801

- (Exam Topic 2)

An organization with a large number of applications wants to establish a security risk assessment program. Which of the following would provide the MOST useful information when determining the frequency of risk assessments?

- A. Feedback from end users
- B. Results of a benchmark analysis
- C. Recommendations from internal audit
- D. Prioritization from business owners

**Answer:** D

#### NEW QUESTION 803

- (Exam Topic 2)

Which of the following is MOST important for an organization that wants to reduce IT operational risk?

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

**Answer:** C

#### NEW QUESTION 806

- (Exam Topic 2)

Which of the following risk scenarios would be the GREATEST concern as a result of a single sign-on implementation?

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

**Answer:** B

#### NEW QUESTION 810

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 811

- (Exam Topic 2)

Which of the following is the BEST indicator of the effectiveness of a control action plan's implementation?

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

**Answer:** B

#### NEW QUESTION 816

- (Exam Topic 2)

Which of the following is MOST helpful in developing key risk indicator (KRI) thresholds?

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

**Answer:** A

#### NEW QUESTION 821

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 824

- (Exam Topic 2)

An organization's risk practitioner learns a new third-party system on the corporate network has introduced vulnerabilities that could compromise corporate IT systems. What should the risk practitioner do FIRST?

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

**Answer:** B

#### NEW QUESTION 827

- (Exam Topic 2)

Which of the following is a crucial component of a key risk indicator (KRI) to ensure appropriate action is taken to mitigate risk?

- A. Management intervention
- B. Risk appetite
- C. Board commentary
- D. Escalation triggers

**Answer:** D

#### NEW QUESTION 831

- (Exam Topic 2)

A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?

- A. Review the design of the machine learning model against control objectives.
- B. Adopt the machine learning model as a replacement for current manual access reviews.
- C. Ensure the model assists in meeting regulatory requirements for access controls.
- D. Discourage the use of emerging technologies in key processes.

**Answer:** A

#### NEW QUESTION 834

- (Exam Topic 2)

Which of the following is the MOST important consideration when selecting either a qualitative or quantitative risk analysis?

- A. Expertise in both methodologies
- B. Maturity of the risk management program
- C. Time available for risk analysis
- D. Resources available for data analysis

**Answer:** D

#### NEW QUESTION 836

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 839

- (Exam Topic 2)

A risk practitioner shares the results of a vulnerability assessment for a critical business application with the business manager. Which of the following is the NEXT step?

- A. Develop a risk action plan to address the findings.
- B. Evaluate the impact of the vulnerabilities to the business application.
- C. Escalate the findings to senior management and internal audit.
- D. Conduct a penetration test to validate the vulnerabilities from the findings.

**Answer: B**

#### NEW QUESTION 841

- (Exam Topic 2)

Which of the following is a detective control?

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

**Answer: B**

#### NEW QUESTION 842

- (Exam Topic 2)

An organization plans to migrate sensitive information to a public cloud infrastructure. Which of the following is the GREATEST security risk in this scenario?

- A. Data may be commingled with other tenants' data.
- B. System downtime does not meet the organization's thresholds.
- C. The infrastructure will be managed by the public cloud administrator.
- D. The cloud provider is not independently certified.

**Answer: A**

#### NEW QUESTION 844

- (Exam Topic 2)

An organization has granted a vendor access to its data in order to analyze customer behavior. Which of the following would be the MOST effective control to mitigate the risk of customer data leakage?

- A. Enforce criminal background checks.
- B. Mask customer data fields.
- C. Require vendor to sign a confidentiality agreement.
- D. Restrict access to customer data on a "need to know" basis.

**Answer: D**

#### NEW QUESTION 847

.....



## 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/>