

## CRISC Dumps

### Certified in Risk and Information Systems Control

<https://www.certleader.com/CRISC-dumps.html>



**NEW QUESTION 1**

- (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 2**

- (Exam Topic 4)

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

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

**Answer: A**

**NEW QUESTION 3**

- (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 4**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 5**

- (Exam Topic 4)

Using key risk indicators (KRIs) to illustrate changes in the risk profile PRIMARILY helps to:

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

**Answer: A**

**NEW QUESTION 6**

- (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 7**

- (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 8**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 9**

- (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 10**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 10**

- (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 13**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 18**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 19**

- (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 23

- (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 26

- (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 28

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 32

- (Exam Topic 4)

Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

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

**Answer: A**

#### NEW QUESTION 36

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 37

- (Exam Topic 4)

Which of the following is the BEST approach for an organization in a heavily regulated industry to comprehensively test application functionality?

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

**Answer: D**

**NEW QUESTION 42**

- (Exam Topic 4)

Which of the following is the MOST important consideration when developing risk strategies?

- A. Organization's industry sector
- B. Long-term organizational goals
- C. Concerns of the business process owners
- D. History of risk events

**Answer:** B

**NEW QUESTION 47**

- (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 52**

- (Exam Topic 4)

Which of the following is the BEST method to maintain a common view of IT risk within an organization?

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

**Answer:** C

**NEW QUESTION 54**

- (Exam Topic 4)

Which of the following provides the BEST assurance of the effectiveness of vendor security controls?

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

**Answer:** C

**NEW QUESTION 58**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 61**

- (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 62**

- (Exam Topic 4)

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

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

**Answer:**

C

**NEW QUESTION 64**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 65**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 68**

- (Exam Topic 3)

Which of the following provides the BEST evidence that a selected risk treatment plan is effective?

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

**Answer: D**

**NEW QUESTION 73**

- (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 77**

- (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 79**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 81**

- (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 85

- (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 88

- (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 89

- (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 90

- (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 91

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 95

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 98

- (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 99**

- (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 100**

- (Exam Topic 3)

The MOST important reason for implementing change control procedures is to ensure:

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

**Answer:** A

**NEW QUESTION 103**

- (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 107**

- (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 109**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 111**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 114**



- (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 116**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 119**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 123**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 125**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 129**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 134**

- (Exam Topic 3)

Reviewing historical risk events is MOST useful for which of the following processes within the risk management life cycle?

- A. Risk monitoring
- B. Risk mitigation
- C. Risk aggregation
- D. Risk assessment

**Answer: D**

**NEW QUESTION 137**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 138**

- (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 140**

- (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 144**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 147**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 152**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 153**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 157**

- (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 160**

- (Exam Topic 3)

Which of the following should be management's PRIMARY consideration when approving risk response action plans?

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

**Answer:** C

**NEW QUESTION 165**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 169**

- (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 172**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 176**

- (Exam Topic 3)

Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

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

**Answer:** B

**NEW QUESTION 180**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 181**

- (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 185**

- (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 187**

- (Exam Topic 3)

Which of the following is the GREATEST risk associated with the misclassification of data?

- A. inadequate resource allocation
- B. Data disruption
- C. Unauthorized access
- D. Inadequate retention schedules

**Answer:** A

**NEW QUESTION 189**

- (Exam Topic 3)

Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures)?

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

**Answer:** D

**NEW QUESTION 194**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 197**

- (Exam Topic 3)

Which of the following is the MOST important consideration when sharing risk management updates with executive management?

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

**Answer:** D

**NEW QUESTION 200**

- (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 202**

- (Exam Topic 3)

Who should be accountable for monitoring the control environment to ensure controls are effective?

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

**Answer:** A

**NEW QUESTION 203**

- (Exam Topic 3)

Which of the following BEST facilitates the alignment of IT risk management with enterprise risk management (ERM)?

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

**Answer:** C

**NEW QUESTION 206**

- (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 208**

- (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 213**

- (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 216**

- (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 220**

- (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 223**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 224**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 226**

- (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 230**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 234**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 238**

- (Exam Topic 4)

Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

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

**Answer:** A



**NEW QUESTION 242**

- (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 247**

- (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 248**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 250**

- (Exam Topic 4)

An organization has completed a risk assessment of one of its service providers. Who should be accountable for ensuring that risk responses are implemented?

- A. IT risk practitioner
- B. Third-party security team
- C. The relationship owner
- D. Legal representation of the business

**Answer:** C

**NEW QUESTION 252**

- (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 257**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 258**

- (Exam Topic 4)

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

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

**Answer:**

A

**NEW QUESTION 261**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 265**

- (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 269**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 274**

- (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 279**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 282**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 285**

- (Exam Topic 4)

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

- A. To support decision-making for risk response
- B. To hold risk owners accountable for risk action plans
- C. To secure resourcing for risk treatment efforts

D. To enable senior management to compile a risk profile

**Answer:** A

**NEW QUESTION 287**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 288**

- (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 290**

- (Exam Topic 4)

Following an acquisition, the acquiring company's risk practitioner has been asked to update the organization's IT risk profile. What is the MOST important information to review from the acquired company to facilitate this task?

- A. Internal and external audit reports
- B. Risk disclosures in financial statements
- C. Risk assessment and risk register
- D. Business objectives and strategies

**Answer:** C

**NEW QUESTION 293**

- (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 296**

- (Exam Topic 4)

Which of the following BEST enables effective IT control implementation?

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

**Answer:** B

**NEW QUESTION 297**

- (Exam Topic 4)

Which of the following contributes MOST to the effective implementation of risk responses?

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

**Answer:** A

**NEW QUESTION 298**

- (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 300**

- (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 305**

- (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 308**

- (Exam Topic 4)

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

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

**Answer:** A

#### **NEW QUESTION 310**

- (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 313**

- (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 317**

- (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 318**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 320**

- (Exam Topic 4)

An organization control environment is MOST effective when:

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

**Answer:** B

**NEW QUESTION 323**

- (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 327**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 330**

- (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 332**

- (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 336**

- (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 341**

- (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 343**

- (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 346**

- (Exam Topic 4)

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

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

**Answer: A**

**NEW QUESTION 347**

- (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 348**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 351**

- (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 354**

- (Exam Topic 4)

Which of the following is the BEST method of creating risk awareness in an organization?

- A. Marking the risk register available to project stakeholders



- B. Ensuring senior management commitment to risk training
- C. Providing regular communication to risk managers
- D. Appointing the risk manager from the business units

**Answer:** B

**NEW QUESTION 359**

- (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 360**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 365**

- (Exam Topic 4)

Which of the following is the BEST way to protect sensitive data from administrators within a public cloud?

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

**Answer:** D

**NEW QUESTION 369**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 372**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 375**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 378**

- (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 382**

- (Exam Topic 4)

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

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

**Answer:** B

#### **NEW QUESTION 383**

- (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 387**

- (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 392**

- (Exam Topic 4)

Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

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

**Answer:** A

#### **NEW QUESTION 393**

- (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 398**

- (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 400**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 404**

- (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 407**

- (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 410**

- (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 413**

- (Exam Topic 4)

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

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

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

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

**Answer: B**

#### NEW QUESTION 415

- (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 416

- (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 417

- (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 421

- (Exam Topic 3)

After a high-profile systems breach at an organization's key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared

the following set of assessments:

Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

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

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

**Answer:** A

#### NEW QUESTION 424

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 427

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 428

- (Exam Topic 3)

When an organization's disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?

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

**Answer:** B

#### NEW QUESTION 433

- (Exam Topic 3)

When developing a risk awareness training program, which of the following training topics would BEST facilitate a thorough understanding of risk scenarios?

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

**Answer:** D

#### NEW QUESTION 434

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 436**

- (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 438**

- (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 439**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 440**

- (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 442**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 444**

- (Exam Topic 3)

A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

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

**Answer:** A

**NEW QUESTION 445**

- (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 447**

- (Exam Topic 3)

The BEST indication that risk management is effective is when risk has been reduced to meet:

- A. risk levels.
- B. risk budgets.
- C. risk appetite.
- D. risk capacity.

**Answer: C**

**NEW QUESTION 450**

- (Exam Topic 3)

Which of the following should a risk practitioner recommend FIRST when an increasing trend of risk events and subsequent losses has been identified?

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

**Answer: C**

**NEW QUESTION 453**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 458**

- (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 463**

- (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 468**

- (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 470**

- (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 472**

- (Exam Topic 3)

To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:

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

**Answer:** A

**NEW QUESTION 475**

- (Exam Topic 3)

Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?

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

**Answer:** B

**NEW QUESTION 476**

- (Exam Topic 3)

When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction based on:

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

**Answer:** A

**NEW QUESTION 479**

- (Exam Topic 3)

Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

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

**Answer:** B

**NEW QUESTION 483**

- (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 487**

- (Exam Topic 3)

The MOST important consideration when selecting a control to mitigate an identified risk is whether:

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

**Answer:** A

**NEW QUESTION 491**

- (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 496**

- (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 497**

- (Exam Topic 3)

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

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

**Answer:** C

#### **NEW QUESTION 499**

- (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 500**

- (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 501**

- (Exam Topic 2)

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

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

**Answer:** D

#### **NEW QUESTION 504**

- (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 506**

- (Exam Topic 2)

Which of the following BEST measures the efficiency of an incident response process?

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

**Answer:** C

**NEW QUESTION 511**

- (Exam Topic 2)

A risk practitioner notices that a particular key risk indicator (KRI) has remained below its established trigger point for an extended period of time. Which of the following should be done FIRST?

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

**Answer:** A

**NEW QUESTION 514**

- (Exam Topic 2)

IT disaster recovery point objectives (RPOs) should be based on the:

- A. maximum tolerable downtime.
- B. maximum tolerable loss of data.
- C. need of each business unit.
- D. type of business.

**Answer:** C

**NEW QUESTION 516**

- (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 517**

- (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 521**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 525**

- (Exam Topic 2)

Which of The following is the MOST relevant information to include in a risk management strategy?

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

**Answer:** D

**NEW QUESTION 529**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 534**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 535**

- (Exam Topic 2)

Who is accountable for risk treatment?

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

**Answer:** D

**NEW QUESTION 540**

- (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 541**

- (Exam Topic 2)

During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

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

**Answer:** A

**NEW QUESTION 544**

- (Exam Topic 2)

When assessing the maturity level of an organization's risk management framework, which of the following deficiencies should be of GREATEST concern to a risk practitioner?

- A. Unclear organizational risk appetite
- B. Lack of senior management participation
- C. Use of highly customized control frameworks
- D. Reliance on qualitative analysis methods

**Answer:** C

**NEW QUESTION 547**

- (Exam Topic 2)

Who should be responsible for strategic decisions on risk management?

- A. Chief information officer (CIO)

- B. Executive management team
- C. Audit committee
- D. Business process owner

**Answer:** B

**NEW QUESTION 551**

- (Exam Topic 2)

Which of the following statements in an organization's current risk profile report is cause for further action by senior management?

- A. Key performance indicator (KPI) trend data is incomplete.
- B. New key risk indicators (KRIs) have been established.
- C. Key performance indicators (KPIs) are outside of targets.
- D. Key risk indicators (KRIs) are lagging.

**Answer:** B

**NEW QUESTION 553**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 557**

- (Exam Topic 2)

Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?

- A. Facilitating risk-aware decision making by stakeholders
- B. Demonstrating management commitment to mitigate risk
- C. Closing audit findings on a timely basis
- D. Ensuring compliance to industry standards

**Answer:** A

**NEW QUESTION 559**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 564**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 567**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 571**

- (Exam Topic 2)



What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

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

**Answer: B**

#### NEW QUESTION 573

- (Exam Topic 2)

Which of the following is MOST essential for an effective change control environment?

- A. Business management approval of change requests
- B. Separation of development and production environments
- C. Requirement of an implementation rollback plan
- D. IT management review of implemented changes

**Answer: A**

#### NEW QUESTION 578

- (Exam Topic 2)

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

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

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

**Answer: A**

#### NEW QUESTION 579

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 580

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 581

- (Exam Topic 2)

The FIRST task when developing a business continuity plan should be to:

- A. determine data backup and recovery availability at an alternate site.
- B. identify critical business functions and resources.
- C. define roles and responsibilities for implementation.
- D. identify recovery time objectives (RTOs) for critical business applications.

**Answer: B**

#### NEW QUESTION 582

- (Exam Topic 2)

Which of the following is the BEST way to ensure ongoing control effectiveness?

- A. Establishing policies and procedures
- B. Periodically reviewing control design
- C. Measuring trends in control performance
- D. Obtaining management control attestations

**Answer: C**

#### **NEW QUESTION 587**

- (Exam Topic 2)

The BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability remediation program is the number of:

- A. vulnerability scans.
- B. recurring vulnerabilities.
- C. vulnerabilities remediated,
- D. new vulnerabilities identified.

**Answer: C**

#### **NEW QUESTION 589**

- (Exam Topic 2)

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

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

**Answer: A**

#### **NEW QUESTION 594**

- (Exam Topic 2)

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

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

**Answer: B**

#### **NEW QUESTION 595**

- (Exam Topic 2)

A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

- A. Recommend avoiding the risk.
- B. Validate the risk response with internal audit.
- C. Update the risk register.
- D. Evaluate outsourcing the process.

**Answer: C**

#### **NEW QUESTION 597**

- (Exam Topic 2)

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

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

**Answer: B**

#### **NEW QUESTION 599**

- (Exam Topic 2)

The annualized loss expectancy (ALE) method of risk analysis:

- A. helps in calculating the expected cost of controls
- B. uses qualitative risk rankings such as low, medium and high.
- C. medium and high.
- D. can be used in a cost-benefit analysis
- E. can be used to determine the indirect business impact.

**Answer: C**

**NEW QUESTION 602**

- (Exam Topic 2)

Implementing which of the following will BEST help ensure that systems comply with an established baseline before deployment?

- A. Vulnerability scanning
- B. Continuous monitoring and alerting
- C. Configuration management
- D. Access controls and active logging

**Answer:** C

**NEW QUESTION 607**

- (Exam Topic 2)

Which of the following should be the PRIMARY objective of a risk awareness training program?

- A. To enable risk-based decision making
- B. To promote awareness of the risk governance function
- C. To clarify fundamental risk management principles
- D. To ensure sufficient resources are available

**Answer:** A

**NEW QUESTION 611**

- (Exam Topic 2)

A risk practitioner is reviewing the status of an action plan to mitigate an emerging IT risk and finds the risk level has increased. The BEST course of action would be to:

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

**Answer:** D

**NEW QUESTION 613**

- (Exam Topic 2)

An organization is planning to outsource its payroll function to an external service provider Which of the following should be the MOST important consideration when selecting the provider?

- A. Disaster recovery plan (DRP) of the system
- B. Right to audit the provider
- C. Internal controls to ensure data privacy
- D. Transparency of key performance indicators (KPIs)

**Answer:** C

**NEW QUESTION 618**

- (Exam Topic 2)

Which of the following will be MOST effective to mitigate the risk associated with the loss of company data stored on personal devices?

- A. An acceptable use policy for personal devices
- B. Required user log-on before synchronizing data
- C. Enforced authentication and data encryption
- D. Security awareness training and testing

**Answer:** C

**NEW QUESTION 622**

- (Exam Topic 2)

Which of the following can be used to assign a monetary value to risk?

- A. Annual loss expectancy (ALE)
- B. Business impact analysis
- C. Cost-benefit analysis
- D. Inherent vulnerabilities

**Answer:** A

**NEW QUESTION 624**

- (Exam Topic 2)

Which of the following would prompt changes in key risk indicator (KRI) thresholds?

- A. Changes to the risk register
- B. Changes in risk appetite or tolerance
- C. Modification to risk categories
- D. Knowledge of new and emerging threats

**Answer:** B

**NEW QUESTION 625**

- (Exam Topic 2)

An organization striving to be on the leading edge in regard to risk monitoring would MOST likely implement:

- A. procedures to monitor the operation of controls.
- B. a tool for monitoring critical activities and controls.
- C. real-time monitoring of risk events and control exceptions.
- D. monitoring activities for all critical assets.
- E. Perform a controls assessment.

**Answer:** C

**NEW QUESTION 627**

- (Exam Topic 2)

The risk associated with a high-risk vulnerability in an application is owned by the:

- A. security department.
- B. business unit
- C. vendor.
- D. IT department.

**Answer:** B

**NEW QUESTION 630**

- (Exam Topic 2)

Which of the following is the MOST important consideration when determining whether to accept residual risk after security controls have been implemented on a critical system?

- A. Cost versus benefit of additional mitigating controls
- B. Annualized loss expectancy (ALE) for the system
- C. Frequency of business impact
- D. Cost of the Information control system

**Answer:** A

**NEW QUESTION 634**

- (Exam Topic 2)

Which of the following should a risk practitioner do FIRST when an organization decides to use a cloud service?

- A. Review the vendor selection process and vetting criteria.
- B. Assess whether use of service falls within risk tolerance thresholds.
- C. Establish service level agreements (SLAs) with the vendor.
- D. Check the contract for appropriate security risk and control provisions.

**Answer:** D

**NEW QUESTION 639**

- (Exam Topic 2)

A risk practitioner has observed that risk owners have approved a high number of exceptions to the information security policy. Which of the following should be the risk practitioner's GREATEST concern?

- A. Security policies are being reviewed infrequently.
- B. Controls are not operating efficiently.
- C. Vulnerabilities are not being mitigated
- D. Aggregate risk is approaching the tolerance threshold

**Answer:** D

**NEW QUESTION 642**

- (Exam Topic 2)

The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:

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

**Answer:** B

**NEW QUESTION 643**

- (Exam Topic 2)

Who is responsible for IT security controls that are outsourced to an external service provider?

- A. Organization's information security manager
- B. Organization's risk function
- C. Service provider's IT management
- D. Service provider's information security manager

**Answer:** B

**NEW QUESTION 648**

- (Exam Topic 2)

Following a significant change to a business process, a risk practitioner believes the associated risk has been reduced. The risk practitioner should advise the risk owner to FIRST

- A. review the key risk indicators.
- B. conduct a risk analysis.
- C. update the risk register
- D. reallocate risk response resources.

**Answer:** A

**NEW QUESTION 651**

- (Exam Topic 2)

The BEST criteria when selecting a risk response is the:

- A. capability to implement the response
- B. importance of IT risk within the enterprise
- C. effectiveness of risk response options
- D. alignment of response to industry standards

**Answer:** C

**NEW QUESTION 656**

- (Exam Topic 2)

The maturity of an IT risk management program is MOST influenced by:

- A. the organization's risk culture
- B. benchmarking results against similar organizations
- C. industry-specific regulatory requirements
- D. expertise available within the IT department

**Answer:** A

**NEW QUESTION 659**

- (Exam Topic 2)

A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

- A. Determine changes in the risk level.
- B. Outsource the vulnerability management process.
- C. Review the patch management process.
- D. Add agenda item to the next risk committee meeting.

**Answer:** C

**NEW QUESTION 660**

- (Exam Topic 2)

Which of the following is the PRIMARY objective for automating controls?

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

**Answer:** A

**NEW QUESTION 663**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 667**

- (Exam Topic 2)

During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?

- A. Communicate the decision to the risk owner for approval
- B. Seek approval from the previous action plan manager.
- C. Identify an owner for the new control.
- D. Modify the action plan in the risk register.

**Answer:** A

#### NEW QUESTION 670

- (Exam Topic 2)

Which of the following would BEST enable a risk practitioner to embed risk management within the organization?

- A. Provide risk management feedback to key stakeholders.
- B. Collect and analyze risk data for report generation.
- C. Monitor and prioritize risk data according to the heat map.
- D. Engage key stakeholders in risk management practices.

**Answer:** D

#### NEW QUESTION 675

- (Exam Topic 2)

Which of the following is the PRIMARY benefit of identifying and communicating with stakeholders at the onset of an IT risk assessment?

- A. Obtaining funding support
- B. Defining the risk assessment scope
- C. Selecting the risk assessment framework
- D. Establishing inherent risk

**Answer:** B

#### NEW QUESTION 677

- (Exam Topic 2)

An organization has received notification that it is a potential victim of a cybercrime that may have compromised sensitive customer data. What should be The FIRST course of action?

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

**Answer:** A

#### NEW QUESTION 681

- (Exam Topic 2)

Which of the following requirements is MOST important to include in an outsourcing contract to help ensure sensitive data stored with a service provider is secure?

- A. A third-party assessment report of control environment effectiveness must be provided at least annually.
- B. Incidents related to data loss must be reported to the organization immediately after they occur.
- C. Risk assessment results must be provided to the organization at least annually.
- D. A cyber insurance policy must be purchased to cover data loss events.

**Answer:** A

#### NEW QUESTION 682

- (Exam Topic 2)

Which of the following is MOST helpful in determining the effectiveness of an organization's IT risk mitigation efforts?

- A. Assigning identification dates for risk scenarios in the risk register
- B. Updating impact assessments for risk scenario
- C. Verifying whether risk action plans have been completed
- D. Reviewing key risk indicators (KRIS)

**Answer:** D

#### NEW QUESTION 687

- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to consider when evaluating plans for changes to IT services?

- A. Change testing schedule
- B. Impact assessment of the change
- C. Change communication plan
- D. User acceptance testing (UAT)

**Answer:** B



**NEW QUESTION 688**

- (Exam Topic 2)

During the control evaluation phase of a risk assessment, it is noted that multiple controls are ineffective. Which of the following should be the risk practitioner's FIRST course of action?

- A. Recommend risk remediation of the ineffective controls.
- B. Compare the residual risk to the current risk appetite.
- C. Determine the root cause of the control failures.
- D. Escalate the control failures to senior management.

**Answer: C**

**NEW QUESTION 693**

- (Exam Topic 2)

The PRIMARY purpose of vulnerability assessments is to:

- A. provide clear evidence that the system is sufficiently secure.
- B. determine the impact of potential threats.
- C. test intrusion detection systems (IDS) and response procedures.
- D. detect weaknesses that could lead to system compromise.

**Answer: D**

**NEW QUESTION 695**

- (Exam Topic 2)

An organization's HR department has implemented a policy requiring staff members to take a minimum of five consecutive days leave per year to mitigate the risk of malicious insider activities. Which of the following is the BEST key performance indicator (KPI) of the effectiveness of this policy?

- A. Number of malicious activities occurring during staff members leave
- B. Percentage of staff members seeking exception to the policy
- C. Percentage of staff members taking leave according to the policy
- D. Financial loss incurred due to malicious activities during staff members' leave

**Answer: B**

**NEW QUESTION 698**

- (Exam Topic 2)

An IT license audit has revealed that there are several unlicensed copies of software to:

- A. immediately uninstall the unlicensed software from the laptops
- B. centralize administration rights on laptops so that installations are controlled
- C. report the issue to management so appropriate action can be taken.
- D. procure the requisite licenses for the software to minimize business impact.

**Answer: B**

**NEW QUESTION 701**

- (Exam Topic 2)

An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

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

**Answer: B**

**NEW QUESTION 706**

- (Exam Topic 2)

An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:

- A. identifying risk scenarios.
- B. determining the risk strategy.
- C. calculating impact and likelihood.
- D. completing the controls catalog.

**Answer: A**

**NEW QUESTION 708**

- (Exam Topic 2)

Who is MOST likely to be responsible for the coordination between the IT risk strategy and the business risk strategy?

- A. Chief financial officer
- B. Information security director
- C. Internal audit director

D. Chief information officer

**Answer:** B

**NEW QUESTION 709**

- (Exam Topic 2)

Which of the following is MOST effective in continuous risk management process improvement?

- A. Periodic assessments
- B. Change management
- C. Awareness training
- D. Policy updates

**Answer:** A

**NEW QUESTION 713**

- (Exam Topic 2)

A payroll manager discovers that fields in certain payroll reports have been modified without authorization. Which of the following control weaknesses could have contributed MOST to this problem?

- A. The user requirements were not documented.
- B. Payroll files were not under the control of a librarian.
- C. The programmer had access to the production programs.
- D. The programmer did not involve the user in testing.

**Answer:** B

**NEW QUESTION 718**

- (Exam Topic 2)

Who should be responsible for implementing and maintaining security controls?

- A. End user
- B. Internal auditor
- C. Data owner
- D. Data custodian

**Answer:** C

**NEW QUESTION 721**

- (Exam Topic 2)

Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?

- A. Establishing a risk management committee
- B. Updating the organization's risk register to reflect the new threat
- C. Communicating the results of the threat impact analysis
- D. Establishing metrics to assess the effectiveness of the responses

**Answer:** C

**NEW QUESTION 725**

- (Exam Topic 2)

Which of the following would be of GREATEST assistance when justifying investment in risk response strategies?

- A. Total cost of ownership
- B. Resource dependency analysis
- C. Cost-benefit analysis
- D. Business impact analysis

**Answer:** C

**NEW QUESTION 726**

- (Exam Topic 2)

Read" rights to application files in a controlled server environment should be approved by the:

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

**Answer:** A

**NEW QUESTION 727**

- (Exam Topic 2)

A recent audit identified high-risk issues in a business unit though a previous control self-assessment (CSA) had good results. Which of the following is the MOST likely reason for the difference?

- A. The audit had a broader scope than the CSA.
- B. The CSA was not sample-based.
- C. The CSA did not test control effectiveness.
- D. The CSA was compliance-based, while the audit was risk-based.

**Answer:** D

**NEW QUESTION 732**

- (Exam Topic 2)

Which of the following should be the PRIMARY recipient of reports showing the progress of a current IT risk mitigation project?

- A. Senior management
- B. Project manager
- C. Project sponsor
- D. IT risk manager

**Answer:** A

**NEW QUESTION 736**

- (Exam Topic 2)

Which of the following is the MOST important reason to revisit a previously accepted risk?

- A. To update risk ownership
- B. To review the risk acceptance with new stakeholders
- C. To ensure risk levels have not changed
- D. To ensure controls are still operating effectively

**Answer:** C

**NEW QUESTION 737**

- (Exam Topic 2)

An organization has completed a project to implement encryption on all databases that host customer data. Which of the following elements of the risk register should be updated to reflect this change?

- A. Risk likelihood
- B. Inherent risk
- C. Risk appetite
- D. Risk tolerance

**Answer:** B

**NEW QUESTION 738**

- (Exam Topic 2)

Which of the following would BEST help secure online financial transactions from improper users?

- A. Review of log-in attempts
- B. Multi-level authorization
- C. Periodic review of audit trails
- D. Multi-factor authentication

**Answer:** D

**NEW QUESTION 740**

- (Exam Topic 2)

To mitigate the risk of using a spreadsheet to analyze financial data, IT has engaged a third-party vendor to deploy a standard application to automate the process. Which of the following parties should own the risk associated with calculation errors?

- A. business owner
- B. IT department
- C. Risk manager
- D. Third-party provider

**Answer:** A

**NEW QUESTION 742**

- (Exam Topic 2)

Before implementing instant messaging within an organization using a public solution, which of the following should be in place to mitigate data leakage risk?

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

**Answer:** D

**NEW QUESTION 746**

- (Exam Topic 2)

Who is PRIMARILY accountable for risk treatment decisions?

- A. Risk owner
- B. Business manager
- C. Data owner
- D. Risk manager

**Answer:** A

**NEW QUESTION 748**

- (Exam Topic 2)

Which of the following is the MOST effective way to integrate business risk management with IT operations?

- A. Perform periodic IT control self-assessments.
- B. Require a risk assessment with change requests.
- C. Provide security awareness training.
- D. Perform periodic risk assessments.

**Answer:** D

**NEW QUESTION 750**

- (Exam Topic 2)

Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?

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

**Answer:** A

**NEW QUESTION 751**

- (Exam Topic 2)

The MOST significant benefit of using a consistent risk ranking methodology across an organization is that it enables:

- A. allocation of available resources
- B. clear understanding of risk levels
- C. assignment of risk to the appropriate owners
- D. risk to be expressed in quantifiable terms

**Answer:** B

**NEW QUESTION 754**

- (Exam Topic 2)

Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

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

**Answer:** B

**NEW QUESTION 755**

- (Exam Topic 2)

A large organization is replacing its enterprise resource planning (ERP) system and has decided not to deploy the payroll module of the new system. Instead, the current payroll system will continue to be used. Of the following, who should own the risk if the ERP and payroll system fail to operate as expected?

- A. The business owner
- B. The ERP administrator
- C. The project steering committee
- D. The IT project manager

**Answer:** A

**NEW QUESTION 758**

- (Exam Topic 2)

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

- A. The scenarios are based on industry best practice.
- B. The scenarios focus on current vulnerabilities.
- C. The scenarios are relevant to the organization.
- D. The scenarios include technical consequences.

**Answer:** C

**NEW QUESTION 762**

- (Exam Topic 2)

Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

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

**Answer:** D

**NEW QUESTION 765**

- (Exam Topic 2)

An organization has engaged a third party to provide an Internet gateway encryption service that protects sensitive data uploaded to a cloud service. This is an example of risk:

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

**Answer:** A

**NEW QUESTION 767**

- (Exam Topic 2)

Which of the following should be initiated when a high number of noncompliant conditions are observed during review of a control procedure?

- A. Disciplinary action
- B. A control self-assessment
- C. A review of the awareness program
- D. Root cause analysis

**Answer:** D

**NEW QUESTION 772**

- (Exam Topic 2)

Which of the following will BEST help an organization evaluate the control environment of several third-party vendors?

- A. Review vendors' internal risk assessments covering key risk and controls.
- B. Obtain independent control reports from high-risk vendors.
- C. Review vendors performance metrics on quality and delivery of processes.
- D. Obtain vendor references from third parties.

**Answer:** B

**NEW QUESTION 773**

- (Exam Topic 2)

During the initial risk identification process for a business application, it is MOST important to include which of the following stakeholders?

- A. Business process owners
- B. Business process consumers
- C. Application architecture team
- D. Internal audit

**Answer:** A

**NEW QUESTION 774**

- (Exam Topic 2)

A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?

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

**Answer:** B

**NEW QUESTION 778**

- (Exam Topic 2)

After mapping generic risk scenarios to organizational security policies, the NEXT course of action should be to:

- A. record risk scenarios in the risk register for analysis.
- B. validate the risk scenarios for business applicability.
- C. reduce the number of risk scenarios to a manageable set.
- D. perform a risk analysis on the risk scenarios.

**Answer:** B

**NEW QUESTION 783**

- (Exam Topic 2)

Which of the following is the MOST important enabler of effective risk management?

- A. User awareness of policies and procedures
- B. Implementation of proper controls
- C. Senior management support
- D. Continuous monitoring of threats and vulnerabilities

**Answer:** C

**NEW QUESTION 784**

- (Exam Topic 2)

An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?

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

**Answer:** A

**NEW QUESTION 787**

- (Exam Topic 2)

Which of the following BEST contributes to the implementation of an effective risk response action plan?

- A. An IT tactical plan
- B. Disaster recovery and continuity testing
- C. Assigned roles and responsibilities
- D. A business impact analysis

**Answer:** C

**NEW QUESTION 792**

- (Exam Topic 2)

Of the following, who should be responsible for determining the inherent risk rating of an application?

- A. Application owner
- B. Senior management
- C. Risk practitioner
- D. Business process owner

**Answer:** C

**NEW QUESTION 797**

- (Exam Topic 2)

An organization is increasingly concerned about loss of sensitive data and asks the risk practitioner to assess the current risk level. Which of the following should the risk practitioner do FIRST?

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

**Answer:** D

**NEW QUESTION 800**

- (Exam Topic 2)

Which of the following presents the GREATEST challenge for an IT risk practitioner who wants to report on trends in historical IT risk levels?

- A. Qualitative measures for potential loss events
- B. Changes in owners for identified IT risk scenarios
- C. Changes in methods used to calculate probability
- D. Frequent use of risk acceptance as a treatment option

**Answer:** A

**NEW QUESTION 804**

- (Exam Topic 2)

A risk owner should be the person accountable for:

- A. the risk management process



- B. managing controls.
- C. implementing actions.
- D. the business process.

**Answer:** C

**NEW QUESTION 809**

- (Exam Topic 2)

Risk aggregation in a complex organization will be MOST successful when:

- A. using the same scales in assessing risk
- B. utilizing industry benchmarks
- C. using reliable qualitative data for risk Hems
- D. including primarily low level risk factors

**Answer:** A

**NEW QUESTION 812**

- (Exam Topic 2)

The effectiveness of a control has decreased. What is the MOST likely effect on the associated risk?

- A. The risk impact changes.
- B. The risk classification changes.
- C. The inherent risk changes.
- D. The residual risk changes.

**Answer:** D

**NEW QUESTION 814**

- (Exam Topic 2)

An upward trend in which of the following metrics should be of MOST concern?

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

**Answer:** C

**NEW QUESTION 816**

- (Exam Topic 2)

When prioritizing risk response, management should FIRST:

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

**Answer:** C

**NEW QUESTION 819**

- (Exam Topic 2)

A large organization needs to report risk at all levels for a new centralized visualization project to reduce cost and improve performance. Which of the following would MOST effectively represent the overall risk of the project to senior management?

- A. Aggregated key performance indicators (KPIs)
- B. Key risk indicators (KRIs)
- C. Centralized risk register
- D. Risk heat map

**Answer:** D

**NEW QUESTION 821**

- (Exam Topic 2)

Which of the following BEST reduces the probability of laptop theft?

- A. Cable lock
- B. Acceptable use policy
- C. Data encryption
- D. Asset tag with GPS

**Answer:** A

**NEW QUESTION 825**

- (Exam Topic 1)

Which of the following is the BEST method to ensure a terminated employee's access to IT systems is revoked upon departure from the organization?

- A. Login attempts are reconciled to a list of terminated employees.
- B. A list of terminated employees is generated for reconciliation against current IT access.
- C. A process to remove employee access during the exit interview is implemented.
- D. The human resources (HR) system automatically revokes system access.

**Answer:** D

#### **NEW QUESTION 829**

- (Exam Topic 1)

Which of the following is the MOST important key performance indicator (KPI) to establish in the service level agreement (SLA) for an outsourced data center?

- A. Percentage of systems included in recovery processes
- B. Number of key systems hosted
- C. Average response time to resolve system incidents
- D. Percentage of system availability

**Answer:** C

#### **NEW QUESTION 831**

- (Exam Topic 1)

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

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

**Answer:** B

#### **NEW QUESTION 835**

- (Exam Topic 1)

A global organization is considering the acquisition of a competitor. Senior management has requested a review of the overall risk profile from the targeted organization. Which of the following components of this review would provide the MOST useful information?

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

**Answer:** D

#### **NEW QUESTION 836**

- (Exam Topic 1)

A risk practitioner is assisting with the preparation of a report on the organization's disaster recovery (DR) capabilities. Which information would have the MOST impact on the overall recovery profile?

- A. The percentage of systems meeting recovery target times has increased.
- B. The number of systems tested in the last year has increased.
- C. The number of systems requiring a recovery plan has increased.
- D. The percentage of systems with long recovery target times has decreased.

**Answer:** D

#### **NEW QUESTION 841**

- (Exam Topic 1)

A contract associated with a cloud service provider MUST include:

- A. ownership of responsibilities.
- B. a business recovery plan.
- C. provision for source code escrow.
- D. the providers financial statements.

**Answer:** A

#### **NEW QUESTION 846**

- (Exam Topic 1)

Which of the following is the BEST way to validate the results of a vulnerability assessment?

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

**Answer:** A

**NEW QUESTION 847**

- (Exam Topic 1)

Which of the following is the BEST way for a risk practitioner to help management prioritize risk response?

- A. Align business objectives to the risk profile.
- B. Assess risk against business objectives
- C. Implement an organization-specific risk taxonomy.
- D. Explain risk details to management.

**Answer:** B

**NEW QUESTION 852**

- (Exam Topic 1)

Which of the following is the MOST important requirement for monitoring key risk indicators (KRIs) using log analysis?

- A. Obtaining logs in an easily readable format
- B. Providing accurate logs in a timely manner
- C. Collecting logs from the entire set of IT systems
- D. implementing an automated log analysis tool

**Answer:** B

**NEW QUESTION 855**

- (Exam Topic 1)

The number of tickets to rework application code has significantly exceeded the established threshold. Which of the following would be the risk practitioner's BEST recommendation?

- A. Perform a root cause analysis
- B. Perform a code review
- C. Implement version control software.
- D. Implement training on coding best practices

**Answer:** A

**NEW QUESTION 860**

- (Exam Topic 1)

IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would be MOST helpful?

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

**Answer:** A

**NEW QUESTION 863**

- (Exam Topic 1)

Which of the following changes would be reflected in an organization's risk profile after the failure of a critical patch implementation?

- A. Risk tolerance is decreased.
- B. Residual risk is increased.
- C. Inherent risk is increased.
- D. Risk appetite is decreased

**Answer:** B

**NEW QUESTION 867**

- (Exam Topic 1)

Which of the following would MOST effectively enable a business operations manager to identify events exceeding risk thresholds?

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

**Answer:** A

**NEW QUESTION 870**

- (Exam Topic 1)

Which of the following is the BEST way to identify changes to the risk landscape?

- A. Internal audit reports
- B. Access reviews
- C. Threat modeling
- D. Root cause analysis

**Answer:** C

**NEW QUESTION 874**

- (Exam Topic 1)

The PRIMARY benefit of maintaining an up-to-date risk register is that it helps to:

- A. implement uniform controls for common risk scenarios.
- B. ensure business unit risk is uniformly distributed.
- C. build a risk profile for management review.
- D. quantify the organization's risk appetite.

**Answer:** C

**NEW QUESTION 876**

- (Exam Topic 1)

A risk assessment has identified that departments have installed their own WiFi access points on the enterprise network. Which of the following would be MOST important to include in a report to senior management?

- A. The network security policy
- B. Potential business impact
- C. The WiFi access point configuration
- D. Planned remediation actions

**Answer:** B

**NEW QUESTION 879**

- (Exam Topic 1)

Whether the results of risk analyses should be presented in quantitative or qualitative terms should be based PRIMARILY on the:

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

**Answer:** A

**NEW QUESTION 880**

- (Exam Topic 1)

A risk practitioner has observed that there is an increasing trend of users sending sensitive information by email without using encryption. Which of the following would be the MOST effective approach to mitigate the risk associated with data loss?

- A. Implement a tool to create and distribute violation reports
- B. Raise awareness of encryption requirements for sensitive data.
- C. Block unencrypted outgoing emails which contain sensitive data.
- D. Implement a progressive disciplinary process for email violations.

**Answer:** C

**NEW QUESTION 885**

- (Exam Topic 1)

Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?

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

**Answer:** A

**NEW QUESTION 887**

- (Exam Topic 1)

A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:

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

**Answer:** D

**NEW QUESTION 891**

- (Exam Topic 1)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery plan (DRP)?

- A. Number of users that participated in the DRP testing
- B. Number of issues identified during DRP testing
- C. Percentage of applications that met the RTO during DRP testing
- D. Percentage of issues resolved as a result of DRP testing

**Answer:** B

**NEW QUESTION 895**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CRISC Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CRISC-dumps.html>