



**Isaca**

## **Exam Questions CRISC**

Certified in Risk and Information Systems Control

#### NEW QUESTION 1

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 2

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 3

- (Exam Topic 4)

Which of the following is the BEST way to ensure data is properly sanitized while in cloud storage?

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

**Answer: B**

#### NEW QUESTION 4

- (Exam Topic 4)

During a risk assessment, a key external technology supplier refuses to provide control design and effectiveness information, citing confidentiality concerns. What should the risk practitioner do NEXT?

- A. Escalate the non-cooperation to management
- B. Exclude applicable controls from the assessment.
- C. Review the supplier's contractual obligations.
- D. Request risk acceptance from the business process owner.

**Answer: C**

#### NEW QUESTION 5

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 6

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 7

- (Exam Topic 4)

Which of the following is the MOST effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage?

- A. Enforce sanctions for noncompliance with security procedures.
- B. Conduct organization-wide phishing simulations.

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

**Answer:** B

#### NEW QUESTION 8

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 9

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 10

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 11

- (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 15

- (Exam Topic 4)

Which of the following would be of MOST concern to a risk practitioner reviewing risk action plans for documented IT risk scenarios?

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

**Answer:** B

#### NEW QUESTION 16

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 17

- (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 19

- (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 22

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 27

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 29

- (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 33

- (Exam Topic 4)

Which of the following is MOST important to determine when assessing the potential risk exposure of a loss event involving personal data?

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

**Answer:** C

#### NEW QUESTION 35

- (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 37

- (Exam Topic 4)

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

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

**Answer: D**

#### NEW QUESTION 41

- (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 45

- (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 47

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 51

- (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 54

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 58

- (Exam Topic 3)

The BEST way to improve a risk register is to ensure the register:

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

**Answer:** A

#### NEW QUESTION 59

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 64

- (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 69

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 74

- (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 can be concluded by analyzing the latest vulnerability report for the IT infrastructure?

- A. Likelihood of a threat
- B. Impact of technology risk
- C. Impact of operational risk
- D. Control weakness

**Answer:** C

#### NEW QUESTION 80

- (Exam Topic 3)

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

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



**Answer:** B

**NEW QUESTION 85**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 89**

- (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 92**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 93**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 94**

- (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 97**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 102**

- (Exam Topic 3)

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

- A. Monitoring is only conducted between official hours of business
- B. Employees are informed of how they are being monitored

- C. Reporting on nonproductive employees is sent to management on a scheduled basis
- D. Multiple data monitoring sources are integrated into security incident response procedures

**Answer:** B

#### NEW QUESTION 103

- (Exam Topic 3)

When developing a new risk register, a risk practitioner should focus on which of the following risk management activities?

- A. Risk management strategy planning
- B. Risk monitoring and control
- C. Risk identification
- D. Risk response planning

**Answer:** C

#### NEW QUESTION 106

- (Exam Topic 3)

Which of the following is the MOST important topic to cover in a risk awareness training program for all staff?

- A. Internal and external information security incidents
- B. The risk department's roles and responsibilities
- C. Policy compliance requirements and exceptions process
- D. The organization's information security risk profile

**Answer:** C

#### NEW QUESTION 107

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 109

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 113

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 115

- (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 119

- (Exam Topic 3)

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



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

**Answer:** A

#### NEW QUESTION 122

- (Exam Topic 3)

Which of the following is the PRIMARY benefit of using an entry in the risk register to track the aggregate risk associated with server failure?

- A. It provides a cost-benefit analysis on control options available for implementation.
- B. It provides a view on where controls should be applied to maximize the uptime of servers.
- C. It provides historical information about the impact of individual servers malfunctioning.
- D. It provides a comprehensive view of the impact should the servers simultaneously fail.

**Answer:** D

#### NEW QUESTION 123

- (Exam Topic 3)

Risk acceptance of an exception to a security control would MOST likely be justified when:

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

**Answer:** B

#### NEW QUESTION 127

- (Exam Topic 3)

An IT department originally planned to outsource the hosting of its data center at an overseas location to reduce operational expenses. After a risk assessment, the department has decided to keep the data center in-house. How should the risk treatment response be reflected in the risk register?

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

**Answer:** A

#### NEW QUESTION 128

- (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 133

- (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 138

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 139

- (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 142

- (Exam Topic 3)

Determining if organizational risk is tolerable requires:

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

**Answer: D**

#### NEW QUESTION 143

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 148

- (Exam Topic 3)

Which of the following is the MOST effective way to incorporate stakeholder concerns when developing risk scenarios?

- A. Evaluating risk impact
- B. Establishing key performance indicators (KPIs)
- C. Conducting internal audits
- D. Creating quarterly risk reports

**Answer: A**

#### NEW QUESTION 151

- (Exam Topic 3)

A risk practitioner has been asked to advise management on developing a log collection and correlation strategy. Which of the following should be the MOST important consideration when developing this strategy?

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

**Answer: A**

#### NEW QUESTION 156

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 159

- (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 162

- (Exam Topic 3)

Which of the following scenarios represents a threat?

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

**Answer:** D

#### NEW QUESTION 163

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 164

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 165

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 167

- (Exam Topic 3)

The BEST way to obtain senior management support for investment in a control implementation would be to articulate the reduction in:

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

**Answer:** D

#### NEW QUESTION 172

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 174

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 175**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 176**

- (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 178**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 179**

- (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 182**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 183**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 184**

- (Exam Topic 3)

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

- A. Personal data attributed to a specific data subject is tokenized.
- B. Data protection impact assessments are performed on a regular basis.

- C. Personal data certifications are performed to prevent excessive data collection.
- D. Data retention guidelines are documented, established, and enforced.

**Answer:** B

#### NEW QUESTION 189

- (Exam Topic 3)

Which of the following is the BEST control to detect an advanced persistent threat (APT)?

- A. Utilizing antivirus systems and firewalls
- B. Conducting regular penetration tests
- C. Monitoring social media activities
- D. Implementing automated log monitoring

**Answer:** D

#### NEW QUESTION 194

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 198

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 203

- (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 205

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 208

- (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 212

- (Exam Topic 3)

The PRIMARY objective of a risk identification process is to:

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

**Answer:** B

#### NEW QUESTION 215

- (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 217

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 222

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 224

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 228

- (Exam Topic 3)

What should be the PRIMARY driver for periodically reviewing and adjusting key risk indicators (KRIs)?

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

**Answer:** B

#### NEW QUESTION 232

- (Exam Topic 3)

Analyzing trends in key control indicators (KCIs) BEST enables a risk practitioner to proactively identify impacts on an organization's:

- A. risk classification methods
- B. risk-based capital allocation
- C. risk portfolio
- D. risk culture

**Answer:** C

#### NEW QUESTION 234



- (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 239

- (Exam Topic 3)

Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

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

**Answer: A**

#### NEW QUESTION 242

- (Exam Topic 3)

Which of the following risk management practices BEST facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register?

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

**Answer: D**

#### NEW QUESTION 245

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 247

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 252

- (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 255

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 260

- (Exam Topic 3)

Which of the following controls BEST enables an organization to ensure a complete and accurate IT asset inventory?

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

**Answer: B**

#### NEW QUESTION 261

- (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 265

- (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 269

- (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 271

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 275

- (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 277

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 281**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 284**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 287**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 292**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 293**

- (Exam Topic 3)

An organization is implementing internet of Things (IoT) technology to control temperature and lighting in its headquarters. Which of the following should be of GREATEST concern?

- A. Insufficient network isolation
- B. impact on network performance
- C. insecure data transmission protocols
- D. Lack of interoperability between sensors

**Answer:** D

**NEW QUESTION 297**

- (Exam Topic 4)

The objective of aligning mitigating controls to risk appetite is to ensure that:

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

**Answer:** D

**NEW QUESTION 302**

- (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 305

- (Exam Topic 4)

Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

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

**Answer:** C

#### NEW QUESTION 309

- (Exam Topic 4)

Recovery the objectives (RTOs) should be based on

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

**Answer:** C

#### NEW QUESTION 313

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 317

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 318

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 320

- (Exam Topic 4)

Which of the following BEST enables senior management to compare the ratings of risk scenarios?

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

**Answer:** D

#### NEW QUESTION 323

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 324

- (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 327

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 332

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 333

- (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 336

- (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 339

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 341

- (Exam Topic 4)

Which of the following is the BEST key performance indicator (KPI) to measure how effectively risk management practices are embedded in the project management office (PMO)?

- A. Percentage of projects with key risk accepted by the project steering committee
- B. Reduction in risk policy noncompliance findings
- C. Percentage of projects with developed controls on scope creep
- D. Reduction in audits involving external risk consultants

**Answer: C**

#### NEW QUESTION 346

- (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 350

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 355

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 357

- (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 360

- (Exam Topic 4)

Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

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

**Answer: A**

#### NEW QUESTION 363

- (Exam Topic 4)

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

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



**Answer:** B

**NEW QUESTION 364**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 367**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 369**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 372**

- (Exam Topic 4)

An organization recently configured a new business division Which of the following is MOST likely to be affected?

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

**Answer:** A

**NEW QUESTION 373**

- (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 375**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 380**

- (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 384

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 385

- (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 388

- (Exam Topic 4)

When reviewing the business continuity plan (BCP) of an online sales order system, a risk practitioner notices that the recovery time objective (RTO) has a shorter time than what is defined in the disaster recovery plan (DRP). Which of the following is the BEST way for the risk practitioner to address this concern?

- A. Adopt the RTO defined in the BCR
- B. Update the risk register to reflect the discrepancy.
- C. Adopt the RTO defined in the DRP.
- D. Communicate the discrepancy to the DR manager for follow-up.

**Answer:** D

#### NEW QUESTION 393

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 398

- (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 399

- (Exam Topic 4)

Which of the following is the BEST way to help ensure risk will be managed properly after a business process has been re-engineered?

- A. Reassessing control effectiveness of the process
- B. Conducting a post-implementation review to determine lessons learned
- C. Reporting key performance indicators (KPIs) for core processes
- D. Establishing escalation procedures for anomaly events

**Answer:** A

#### NEW QUESTION 403

- (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 405

- (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 409

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 412

- (Exam Topic 4)

Which of the following is the BEST way to determine whether system settings are in alignment with control baselines?

- A. Configuration validation
- B. Control attestation
- C. Penetration testing
- D. Internal audit review

**Answer:** A

#### NEW QUESTION 413

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 417

- (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 419

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 424

- (Exam Topic 4)

Effective risk communication BEST benefits an organization by:

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

**Answer:** A

#### NEW QUESTION 429

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 433

- (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 434

- (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 438

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 440

- (Exam Topic 4)

It is MOST important that security controls for a new system be documented in:

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

**Answer:** C

#### NEW QUESTION 443

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 446**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 449**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 452**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 456**

- (Exam Topic 4)

The MAIN purpose of selecting a risk response is to.

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

**Answer:** C

**NEW QUESTION 460**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 464**

- (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 467**

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 470

- (Exam Topic 4)

Which of the following will BEST ensure that controls adequately support business goals and objectives?

- A. Using the risk management process
- B. Enforcing strict disciplinary procedures in case of noncompliance
- C. Reviewing results of the annual company external audit
- D. Adopting internationally accepted controls

**Answer:** A

#### NEW QUESTION 473

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 476

- (Exam Topic 4)

A newly incorporated enterprise needs to secure its information assets From a governance perspective which of the following should be done FIRST?

- A. Define information retention requirements and policies
- B. Provide information security awareness training
- C. Establish security management processes and procedures
- D. Establish an inventory of information assets

**Answer:** D

#### NEW QUESTION 481

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 484

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 489

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 492

- (Exam Topic 3)



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

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

**Answer:** D

#### NEW QUESTION 493

- (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 495

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 498

- (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 499

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 501

- (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 503

- (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 506

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 508

- (Exam Topic 3)

An organization's risk register contains a large volume of risk scenarios that senior management considers overwhelming. Which of the following would BEST help to improve the risk register?

- A. Analyzing the residual risk components
- B. Performing risk prioritization
- C. Validating the risk appetite level
- D. Conducting a risk assessment

**Answer: D**

#### NEW QUESTION 513

- (Exam Topic 3)

Prudent business practice requires that risk appetite not exceed:

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

**Answer: C**

#### NEW QUESTION 517

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 519

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 520

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 523

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 527**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 532**

- (Exam Topic 3)

The PRIMARY purpose of IT control status reporting is to:

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

**Answer:** A

**NEW QUESTION 533**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 535**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 538**

- (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 540**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 543**

- (Exam Topic 3)

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

- A. Improved senior management communication
- B. Optimized risk treatment decisions
- C. Enhanced awareness of risk management

D. Improved collaboration among risk professionals

**Answer:** B

**NEW QUESTION 548**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 550**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 553**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 557**

- (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 561**

- (Exam Topic 3)

A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

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

**Answer:** A

**NEW QUESTION 565**

- (Exam Topic 3)

Which of the following will BEST help in communicating strategic risk priorities?

- A. Heat map
- B. Business impact analysis (BIA)
- C. Balanced Scorecard
- D. Risk register

**Answer:** A

**NEW QUESTION 566**

- (Exam Topic 3)

Which of the following is the BEST way for an organization to enable risk treatment decisions?

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

**Answer:** C

#### NEW QUESTION 567

- (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 570

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 571

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 574

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 576

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 580

- (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 582

- (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 583

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 588

- (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 589

- (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 592

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 597

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 598

- (Exam Topic 2)

The PRIMARY benefit of classifying information assets is that it helps to:

- A. communicate risk to senior management
- B. assign risk ownership
- C. facilitate internal audit
- D. determine the appropriate level of control



**Answer:** D

**NEW QUESTION 602**

- (Exam Topic 2)

Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?

- A. Defining expectations in the enterprise risk policy
- B. Increasing organizational resources to mitigate risks
- C. Communicating external audit results
- D. Avoiding risks that could materialize into substantial losses

**Answer:** A

**NEW QUESTION 604**

- (Exam Topic 2)

When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:

- A. risk appetite.
- B. security policies
- C. process maps.
- D. risk tolerance level

**Answer:** B

**NEW QUESTION 605**

- (Exam Topic 2)

Controls should be defined during the design phase of system development because:

- A. it is more cost-effective to determine controls in the early design phase.
- B. structured analysis techniques exclude identification of controls.
- C. structured programming techniques require that controls be designed before coding begins.
- D. technical specifications are defined during this phase.

**Answer:** A

**NEW QUESTION 608**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 610**

- (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 615**

- (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 616**

- (Exam Topic 2)

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

- A. Expertise in both methodologies
- B. Maturity of the risk management program

- C. Time available for risk analysis
- D. Resources available for data analysis

**Answer:** D

#### NEW QUESTION 619

- (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 623

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 628

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 632

- (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 636

- (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 638

- (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 641

- (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 644

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 647

- (Exam Topic 2)

Which of the following is the GREATEST risk associated with the use of data analytics?

- A. Distributed data sources
- B. Manual data extraction
- C. Incorrect data selection
- D. Excessive data volume

**Answer:** C

#### NEW QUESTION 649

- (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 651

- (Exam Topic 2)

Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

- A. Key risk indicators (KRIs)
- B. Data backups
- C. Incident response plan
- D. Cyber insurance

**Answer:** C

#### NEW QUESTION 652

- (Exam Topic 2)

Which of the following BEST promotes commitment to controls?

- A. Assigning control ownership
- B. Assigning appropriate resources
- C. Assigning a quality control review
- D. Performing regular independent control reviews

**Answer:** A

#### NEW QUESTION 657

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 660

- (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 661

- (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 662

- (Exam Topic 2)

The GREATEST concern when maintaining a risk register is that:

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

**Answer: D**

#### NEW QUESTION 664

- (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 669

- (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 671

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk responses have been executed according to their risk action plans?

- A. Risk policy review
- B. Business impact analysis (BIA)
- C. Control catalog
- D. Risk register

**Answer: D**

#### NEW QUESTION 672

- (Exam Topic 2)

A department has been granted an exception to bypass the existing approval process for purchase orders. The risk practitioner should verify the exception has been approved by which of the following?

- A. Internal audit
- B. Control owner
- C. Senior management
- D. Risk manager

**Answer:** B

**NEW QUESTION 674**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 678**

- (Exam Topic 2)

Which of the following is MOST critical to the design of relevant risk scenarios?

- A. The scenarios are based on past incidents.
- B. The scenarios are linked to probable organizational situations.
- C. The scenarios are mapped to incident management capabilities.
- D. The scenarios are aligned with risk management capabilities.

**Answer:** B

**NEW QUESTION 681**

- (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 686**

- (Exam Topic 2)

Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?

- A. The KRIs' source data lacks integrity.
- B. The KRIs are not automated.
- C. The KRIs are not quantitative.
- D. The KRIs do not allow for trend analysis.

**Answer:** A

**NEW QUESTION 690**

- (Exam Topic 2)

Which of the following criteria is MOST important when developing a response to an attack that would compromise data?

- A. The recovery time objective (RTO)
- B. The likelihood of a recurring attack
- C. The organization's risk tolerance
- D. The business significance of the information

**Answer:** D

**NEW QUESTION 691**

- (Exam Topic 2)

A maturity model will BEST indicate:

- A. confidentiality and integrity.
- B. effectiveness and efficiency.
- C. availability and reliability.
- D. certification and accreditation.

**Answer:** B

**NEW QUESTION 695**

- (Exam Topic 2)

It is MOST important to the effectiveness of an IT risk management function that the associated processes are:

- A. aligned to an industry-accepted framework.
- B. reviewed and approved by senior management.

- C. periodically assessed against regulatory requirements.
- D. updated and monitored on a continuous basis.

**Answer:** C

#### NEW QUESTION 697

- (Exam Topic 2)

Which of the following would qualify as a key performance indicator (KPI)?

- A. Aggregate risk of the organization
- B. Number of identified system vulnerabilities
- C. Number of exception requests processed in the past 90 days
- D. Number of attacks against the organization's website

**Answer:** B

#### NEW QUESTION 699

- (Exam Topic 2)

Reviewing which of the following provides the BEST indication of an organizations risk tolerance?

- A. Risk sharing strategy
- B. Risk transfer agreements
- C. Risk policies
- D. Risk assessments

**Answer:** D

#### NEW QUESTION 701

- (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 706

- (Exam Topic 2)

Which of the following would be MOST beneficial as a key risk indicator (KRI)?

- A. Current capital allocation reserves
- B. Negative security return on investment (ROI)
- C. Project cost variances
- D. Annualized loss projections

**Answer:** D

#### NEW QUESTION 708

- (Exam Topic 2)

Within the three lines of defense model, the accountability for the system of internal control resides with:

- A. the chief information officer (CIO).
- B. the board of directors
- C. enterprise risk management
- D. the risk practitioner

**Answer:** B

#### NEW QUESTION 711

- (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 715

- (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 718

- (Exam Topic 2)

Which of the following is the PRIMARY reason for an organization to ensure the risk register is updated regularly?

- A. Risk assessment results are accessible to senior management and stakeholders.
- B. Risk mitigation activities are managed and coordinated.
- C. Key risk indicators (KRIs) are evaluated to validate they are still within the risk threshold.
- D. Risk information is available to enable risk-based decisions.

**Answer:** D

#### NEW QUESTION 721

- (Exam Topic 2)

Which of the following is the MOST important consideration when performing a risk assessment of a fire suppression system within a data center?

- A. Insurance coverage
- B. Onsite replacement availability
- C. Maintenance procedures
- D. Installation manuals

**Answer:** C

#### NEW QUESTION 722

- (Exam Topic 2)

A risk assessment indicates the residual risk associated with a new bring your own device (BYOD) program is within organizational risk tolerance. Which of the following should the risk practitioner recommend be done NEXT?

- A. Implement targeted awareness training for new BYOD users.
- B. Implement monitoring to detect control deterioration.
- C. Identify log sources to monitor BYOD usage and risk impact.
- D. Reduce the risk tolerance level.

**Answer:** B

#### NEW QUESTION 725

- (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 728

- (Exam Topic 2)

To minimize risk in a software development project, when is the BEST time to conduct a risk analysis?

- A. During the business requirement definitions phase
- B. Before periodic steering committee meetings
- C. At each stage of the development life cycle
- D. During the business case development

**Answer:** A

#### NEW QUESTION 729

- (Exam Topic 2)

Which of the following is the BEST way to identify changes in the risk profile of an organization?

- A. Monitor key risk indicators (KRIs).
- B. Monitor key performance indicators (KPIs).
- C. Interview the risk owner.
- D. Conduct a gap analysis

**Answer:** D

#### NEW QUESTION 730

- (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 735

- (Exam Topic 2)

An organization has outsourced its backup and recovery procedures to a third-party cloud provider. Which of the following is the risk practitioner's BEST course of action?

- A. Accept the risk and document contingency plans for data disruption.
- B. Remove the associated risk scenario from the risk register due to avoidance.
- C. Mitigate the risk with compensating controls enforced by the third-party cloud provider.
- D. Validate the transfer of risk and update the register to reflect the change.

**Answer:** C

#### NEW QUESTION 738

- (Exam Topic 2)

An organization is considering adopting artificial intelligence (AI). Which of the following is the risk practitioner's MOST important course of action?

- A. Develop key risk indicators (KRIs).
- B. Ensure sufficient pre-implementation testing.
- C. Identify applicable risk scenarios.
- D. Identify the organization's critical data.

**Answer:** C

#### NEW QUESTION 741

- (Exam Topic 2)

From a risk management perspective, which of the following is the PRIMARY benefit of using automated system configuration validation tools?

- A. Residual risk is reduced.
- B. Staff costs are reduced.
- C. Operational costs are reduced.
- D. Inherent risk is reduced.

**Answer:** C

#### NEW QUESTION 745

- (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 750

- (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 753

- (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 755

- (Exam Topic 2)

Which of the following activities is PRIMARILY the responsibility of senior management?

- A. Bottom-up identification of emerging risks
- B. Categorization of risk scenarios against a standard taxonomy
- C. Prioritization of risk scenarios based on severity
- D. Review of external loss data

**Answer:** C

#### NEW QUESTION 756

- (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 761

- (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 765

- (Exam Topic 2)

An organization has outsourced its lease payment process to a service provider who lacks evidence of compliance with a necessary regulatory standard. Which risk treatment was adopted by the organization?

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

**Answer:** A

#### NEW QUESTION 766

- (Exam Topic 2)

For no apparent reason, the time required to complete daily processing for a legacy application is approaching a risk threshold. Which of the following activities should be performed FIRST?

- A. Temporarily increase the risk threshold.
- B. Suspend processing to investigate the problem.
- C. Initiate a feasibility study for a new application.
- D. Conduct a root-cause analysis.

**Answer:** D

#### NEW QUESTION 770

- (Exam Topic 2)

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

- 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 771

- (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 773**

- (Exam Topic 2)

When communicating changes in the IT risk profile, which of the following should be included to BEST enable stakeholder decision making?

- A. List of recent incidents affecting industry peers
- B. Results of external attacks and related compensating controls
- C. Gaps between current and desired states of the control environment
- D. Review of leading IT risk management practices within the industry

**Answer:** C

**NEW QUESTION 776**

- (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 778**

- (Exam Topic 2)

The MAIN purpose of having a documented risk profile is to:

- A. comply with external and internal requirements.
- B. enable well-informed decision making.
- C. prioritize investment projects.
- D. keep the risk register up-to-date.

**Answer:** B

**NEW QUESTION 783**

- (Exam Topic 2)

Which of the following activities should be performed FIRST when establishing IT risk management processes?

- A. Collect data of past incidents and lessons learned.
- B. Conduct a high-level risk assessment based on the nature of business.
- C. Identify the risk appetite of the organization.
- D. Assess the goals and culture of the organization.

**Answer:** D

**NEW QUESTION 788**

- (Exam Topic 2)

A risk practitioner is reviewing a vendor contract and finds there is no clause to control privileged access to the organization's systems by vendor employees.

Which of the following is the risk practitioner's BEST course of action?

- A. Contact the control owner to determine if a gap in controls exists.
- B. Add this concern to the risk register and highlight it for management review.
- C. Report this concern to the contracts department for further action.
- D. Document this concern as a threat and conduct an impact analysis.

**Answer:** D

**NEW QUESTION 791**

- (Exam Topic 2)

The BEST way to demonstrate alignment of the risk profile with business objectives is through:

- A. risk scenarios.
- B. risk tolerance.
- C. risk policy.
- D. risk appetite.

**Answer:** B

**NEW QUESTION 796**

- (Exam Topic 2)

Which of the following methods would BEST contribute to identifying obscure risk scenarios?

- A. Brainstorming sessions
- B. Control self-assessments

- C. Vulnerability analysis
- D. Monte Carlo analysis

**Answer:** A

#### NEW QUESTION 797

- (Exam Topic 2)

A risk practitioner has been notified that an employee sent an email in error containing customers' personally identifiable information (PII). Which of the following is the risk practitioner's BEST course of action?

- A. Report it to the chief risk officer.
- B. Advise the employee to forward the email to the phishing team.
- C. follow incident reporting procedures.
- D. Advise the employee to permanently delete the email.

**Answer:** C

#### NEW QUESTION 798

- (Exam Topic 2)

What is MOST important for the risk practitioner to understand when creating an initial IT risk register?

- A. Enterprise architecture (EA)
- B. Control environment
- C. IT objectives
- D. Organizational objectives

**Answer:** D

#### NEW QUESTION 803

- (Exam Topic 2)

Which of the following controls would BEST reduce the likelihood of a successful network attack through social engineering?

- A. Automated controls
- B. Security awareness training
- C. Multifactor authentication
- D. Employee sanctions

**Answer:** B

#### NEW QUESTION 805

- (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 809

- (Exam Topic 2)

Which of the following is the MOST important objective of regularly presenting the project risk register to the project steering committee?

- A. To allocate budget for resolution of risk issues
- B. To determine if new risk scenarios have been identified
- C. To ensure the project timeline is on target
- D. To track the status of risk mitigation actions

**Answer:** D

#### NEW QUESTION 811

- (Exam Topic 2)

Which of the following is MOST important to the effective monitoring of key risk indicators (KRIS)?

- A. Updating the threat inventory with new threats
- B. Automating log data analysis
- C. Preventing the generation of false alerts
- D. Determining threshold levels

**Answer:** D

#### NEW QUESTION 814

- (Exam Topic 2)

Which of the following methods is the BEST way to measure the effectiveness of automated information security controls prior to going live?

- A. Testing in a non-production environment
- B. Performing a security control review
- C. Reviewing the security audit report
- D. Conducting a risk assessment

**Answer:** A

#### NEW QUESTION 819

- (Exam Topic 2)

Which of the following is the MOST important data attribute of key risk indicators (KRIs)?

- A. The data is measurable.
- B. The data is calculated continuously.
- C. The data is relevant.
- D. The data is automatically produced.

**Answer:** C

#### NEW QUESTION 820

- (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 825

- (Exam Topic 2)

An organization has raised the risk appetite for technology risk. The MOST likely result would be:

- A. increased inherent risk.
- B. higher risk management cost
- C. decreased residual risk.
- D. lower risk management cost.

**Answer:** D

#### NEW QUESTION 826

- (Exam Topic 2)

A recent internal risk review reveals the majority of core IT application recovery time objectives (RTOs) have exceeded the maximum time defined by the business application owners. Which of the following is MOST likely to change as a result?

- A. Risk forecasting
- B. Risk tolerance
- C. Risk likelihood
- D. Risk appetite

**Answer:** B

#### NEW QUESTION 831

- (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 836

- (Exam Topic 2)

Which of the following BEST indicates that an organizations risk management program is effective?

- A. Fewer security incidents have been reported.
- B. The number of audit findings has decreased.
- C. Residual risk is reduced.
- D. inherent risk is unchanged.

**Answer:** C

#### NEW QUESTION 840



- (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 844

- (Exam Topic 2)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?

- A. Percentage of vulnerabilities remediated within the agreed service level
- B. Number of vulnerabilities identified during the period
- C. Number of vulnerabilities re-opened during the period
- D. Percentage of vulnerabilities escalated to senior management

**Answer: A**

#### NEW QUESTION 848

- (Exam Topic 2)

A control owner identifies that the organization's shared drive contains personally identifiable information (PII) that can be accessed by all personnel. Which of the following is the MOST effective risk response?

- A. Protect sensitive information with access controls.
- B. Implement a data loss prevention (DLP) solution.
- C. Re-communicate the data protection policy.
- D. Implement a data encryption solution.

**Answer: A**

#### NEW QUESTION 850

- (Exam Topic 2)

The implementation of a risk treatment plan will exceed the resources originally allocated for the risk response. Which of the following should be the risk owner's NEXT action?

- A. Perform a risk assessment.
- B. Accept the risk of not implementing.
- C. Escalate to senior management.
- D. Update the implementation plan.

**Answer: C**

#### NEW QUESTION 854

- (Exam Topic 2)

Following a review of a third-party vendor, it is MOST important for an organization to ensure:

- A. results of the review are accurately reported to management.
- B. identified findings are reviewed by the organization.
- C. results of the review are validated by internal audit.
- D. identified findings are approved by the vendor.

**Answer: A**

#### NEW QUESTION 856

- (Exam Topic 2)

An organization has identified that terminated employee accounts are not disabled or deleted within the time required by corporate policy. Unsure of the reason, the organization has decided to monitor the situation for three months to obtain more information. As a result of this decision, the risk has been:

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

**Answer: B**

#### NEW QUESTION 859

- (Exam Topic 2)

Sensitive data has been lost after an employee inadvertently removed a file from the premises, in violation of organizational policy. Which of the following controls MOST likely failed?

- A. Background checks
- B. Awareness training
- C. User access
- D. Policy management

**Answer:** C

**NEW QUESTION 862**

- (Exam Topic 2)

Which of the following will provide the BEST measure of compliance with IT policies?

- A. Evaluate past policy review reports.
- B. Conduct regular independent reviews.
- C. Perform penetration testing.
- D. Test staff on their compliance responsibilities.

**Answer:** C

**NEW QUESTION 865**

- (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 867**

- (Exam Topic 2)

A risk practitioner is reporting on an increasing trend of ransomware attacks in the industry. Which of the following information is MOST important to include to enable an informed response decision by key stakeholders?

- A. Methods of attack progression
- B. Losses incurred by industry peers
- C. Most recent antivirus scan reports
- D. Potential impact of events

**Answer:** D

**NEW QUESTION 868**

- (Exam Topic 2)

IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

- A. the cost associated with each control.
- B. historical risk assessments.
- C. key risk indicators (KRIs).
- D. information from the risk register.

**Answer:** D

**NEW QUESTION 873**

- (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 877**

- (Exam Topic 2)

Which of the following should be included in a risk assessment report to BEST facilitate senior management's understanding of the results?

- A. Benchmarking parameters likely to affect the results
- B. Tools and techniques used by risk owners to perform the assessments
- C. A risk heat map with a summary of risk identified and assessed
- D. The possible impact of internal and external risk factors on the assessment results

**Answer:** C

**NEW QUESTION 881**

- (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 884

- (Exam Topic 2)

The MOST important reason to monitor key risk indicators (KRIs) is to help management:

- A. identify early risk transfer strategies.
- B. lessen the impact of realized risk.
- C. analyze the chain of risk events.
- D. identify the root cause of risk events.

**Answer:** C

#### NEW QUESTION 887

- (Exam Topic 2)

Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

- A. Risk tolerance
- B. Risk appetite
- C. Risk awareness
- D. Risk policy

**Answer:** B

#### NEW QUESTION 889

- (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 893

- (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 895

- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to update when a software upgrade renders an existing key control ineffective?

- A. Audit engagement letter
- B. Risk profile
- C. IT risk register
- D. Change control documentation

**Answer:** C

#### NEW QUESTION 900

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### CRISC Practice Exam Features:

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

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