

# Isaca

## Exam Questions CRISC

Certified in Risk and Information Systems Control



#### NEW QUESTION 1

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 2

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 3

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 4

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 5

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 6

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 7

- (Exam Topic 4)

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

- A. Request a regulatory risk reporting methodology
- B. Require critical success factors (CSFs) for IT risks.

- C. Establish IT-specific compliance objectives
- D. Communicate IT key risk indicators (KRIs) and triggers

**Answer:** A

#### NEW QUESTION 8

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 9

- (Exam Topic 4)

An organization has decided to postpone the assessment and treatment of several risk scenarios because stakeholders are unavailable. As a result of this decision, the risk associated with these new entries has been;

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

**Answer:** C

#### NEW QUESTION 10

- (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 10

- (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 11

- (Exam Topic 4)

Which of the following would provide the MOST useful input when evaluating the appropriateness of risk responses?

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

**Answer:** B

#### NEW QUESTION 15

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 19

- (Exam Topic 4)

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

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

**Answer: D**

#### NEW QUESTION 24

- (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 25

- (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 29

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 33

- (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 38

- (Exam Topic 4)

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

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

**Answer: D**

#### NEW QUESTION 42

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 43**

- (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 46**

- (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 50**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 53**

- (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 58**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 62**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 66**

- (Exam Topic 4)

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 68**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 70**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 71**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 76**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 80**

- (Exam Topic 4)

An organization has allowed several employees to retire early in order to avoid layoffs Many of these employees have been subject matter experts for critical assets Which type of risk is MOST likely to materialize?

- A. Confidentiality breach
- B. Institutional knowledge loss
- C. Intellectual property loss
- D. Unauthorized access

**Answer: B**

**NEW QUESTION 84**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 85**

- (Exam Topic 4)

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

- A. Subscribe to threat intelligence to monitor external attacks.
- B. Apply patches for a newer version of the application.

- C. Segment the application within the existing network.
- D. Increase the frequency of regular system and data backups.

**Answer:** D

**NEW QUESTION 89**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 91**

- (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 94**

- (Exam Topic 3)

A violation of segregation of duties is when the same:

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

**Answer:** D

**NEW QUESTION 95**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 97**

- (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 101**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 103**

- (Exam Topic 3)



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

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

**Answer: D**

#### NEW QUESTION 108

- (Exam Topic 3)

A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

- A. Regulatory requirements may differ in each country.
- B. Data sampling may be impacted by various industry restrictions.
- C. Business advertising will need to be tailored by country.
- D. The data analysis may be ineffective in achieving objectives.

**Answer: A**

#### NEW QUESTION 109

- (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 112

- (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 113

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 116

- (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 117

- (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 119**

- (Exam Topic 3)

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

- A. Key performance indicators (KPIs)
- B. Risk heat maps
- C. Internal audit findings
- D. Periodic penetration testing

**Answer:** A

**NEW QUESTION 121**

- (Exam Topic 3)

Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?

- A. Evaluating the impact to control objectives
- B. Conducting a root cause analysis
- C. Validating the adequacy of current processes
- D. Reconfiguring the IT infrastructure

**Answer:** B

**NEW QUESTION 123**

- (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 124**

- (Exam Topic 3)

Which of the following is the MOST important responsibility of a risk owner?

- A. Testing control design
- B. Accepting residual risk
- C. Establishing business information criteria
- D. Establishing the risk register

**Answer:** C

**NEW QUESTION 129**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 130**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 133**

- (Exam Topic 3)

An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

- A. identify key risk indicators (KRIs) for ongoing monitoring
- B. validate the CTO's decision with the business process owner
- C. update the risk register with the selected risk response
- D. recommend that the CTO revisit the risk acceptance decision.

**Answer:**

A

**NEW QUESTION 136**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 137**

- (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 142**

- (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 145**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 149**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 154**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 156**

- (Exam Topic 3)

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

- A. Whether the affected technology is used within the organization

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

**Answer:** A

**NEW QUESTION 159**

- (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 162**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 167**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 171**

- (Exam Topic 3)

Which of the following should be included in a risk scenario to be used for risk analysis?

- A. Risk appetite
- B. Threat type
- C. Risk tolerance
- D. Residual risk

**Answer:** B

**NEW QUESTION 173**

- (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 175**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 180**

- (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 182**

- (Exam Topic 3)

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

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

**Answer: B**

#### **NEW QUESTION 184**

- (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 188**

- (Exam Topic 3)

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

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

**Answer: B**

#### **NEW QUESTION 190**

- (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 193**

- (Exam Topic 3)

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

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

**Answer: C**

#### **NEW QUESTION 196**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 199**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 200**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 204**

- (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 206**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 209**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 210**

- (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 211**

- (Exam Topic 3)

Winch of the following key control indicators (KCI) BEST indicates whether security requirements are identified and managed throughout a project He cycle?

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

**Answer:**

A

**NEW QUESTION 214**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 217**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 219**

- (Exam Topic 3)

Which of the following will be MOST effective in uniquely identifying the originator of electronic transactions?

- A. Digital signature
- B. Edit checks
- C. Encryption
- D. Multifactor authentication

**Answer: A**

**NEW QUESTION 223**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 225**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 227**

- (Exam Topic 3)

An organization outsources the processing of its payroll data. A risk practitioner identifies a control weakness at the third party that exposes the payroll data. Who should own this risk?

- A. The third party's IT operations manager
- B. The organization's process owner
- C. The third party's chief risk officer (CRO)
- D. The organization's risk practitioner

**Answer: B**

**NEW QUESTION 232**

- (Exam Topic 3)

Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?

- A. Ongoing availability of data
- B. Ability to aggregate data



- C. Ability to predict trends
- D. Availability of automated reporting systems

**Answer:** D

**NEW QUESTION 233**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 237**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 242**

- (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 243**

- (Exam Topic 3)

When updating the risk register after a risk assessment, which of the following is MOST important to include?

- A. Historical losses due to past risk events
- B. Cost to reduce the impact and likelihood
- C. Likelihood and impact of the risk scenario
- D. Actor and threat type of the risk scenario

**Answer:** C

**NEW QUESTION 246**

- (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 248**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 249**

- (Exam Topic 3)

Analyzing trends in key control indicators (KCI)s 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 252**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 254**

- (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 256**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 258**

- (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 259**

- (Exam Topic 3)

The PRIMARY benefit of using a maturity model is that it helps to evaluate the:

- A. capability to implement new processes
- B. evolution of process improvements
- C. degree of compliance with policies and procedures
- D. control requirements.

**Answer:** B

**NEW QUESTION 261**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 263**

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 268

- (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 273

- (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 278

- (Exam Topic 3)

To help identify high-risk situations, an organization should:

- A. continuously monitor the environment.
- B. develop key performance indicators (KPIs).
- C. maintain a risk matrix.
- D. maintain a risk register.

**Answer: A**

#### NEW QUESTION 282

- (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 284

- (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 289

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 290**

- (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 294**

- (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 298**

- (Exam Topic 4)

Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud environment?

- A. Reviewing the results of independent audits
- B. Performing a site visit to the cloud provider's data center
- C. Performing a due diligence review
- D. Conducting a risk workshop with key stakeholders

**Answer: D**

**NEW QUESTION 300**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 303**

- (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 307**

- (Exam Topic 4)

Which of the following will BEST help to ensure the continued effectiveness of the IT risk management function within an organization experiencing high employee turnover?

- A. Well documented policies and procedures
- B. Risk and issue tracking
- C. An IT strategy committee
- D. Change and release management

**Answer: B**

**NEW QUESTION 312**

- (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 314**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 317**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 318**

- (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)

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

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

**Answer:** B

**NEW QUESTION 325**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 329**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 332**

- (Exam Topic 4)

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

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

D. Performing regular reviews and updates to the register

**Answer:** D

**NEW QUESTION 333**

- (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 336**

- (Exam Topic 4)

What is the PRIMARY reason an organization should include background checks on roles with elevated access to production as part of its hiring process?

- A. Reduce internal threats
- B. Reduce exposure to vulnerabilities
- C. Eliminate risk associated with personnel
- D. Ensure new hires have the required skills

**Answer:** C

**NEW QUESTION 341**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 342**

- (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 345**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 346**

- (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 350**

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 353

- (Exam Topic 4)

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

- A. capacity.
- B. appetite.
- C. management capability.
- D. treatment strategy.

**Answer: B**

#### NEW QUESTION 356

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 357

- (Exam Topic 4)

Which of the following is the MOST important course of action for a risk practitioner when reviewing the results of control performance monitoring?

- A. Evaluate changes to the organization's risk profile.
- B. Validate whether the controls effectively mitigate risk.
- C. Confirm controls achieve regulatory compliance.
- D. Analyze appropriateness of key performance indicators (KPIs).

**Answer: D**

#### NEW QUESTION 358

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 361

- (Exam Topic 4)

Which of the following is the MOST important reason to validate that risk responses have been executed as outlined in the risk response plan?

- A. To ensure completion of the risk assessment cycle
- B. To ensure controls are operating effectively
- C. To ensure residual risk is at an acceptable level
- D. To ensure control costs do not exceed benefits

**Answer: A**

#### NEW QUESTION 364

- (Exam Topic 4)

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

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

**Answer: A**



**NEW QUESTION 366**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 368**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 371**

- (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 375**

- (Exam Topic 4)

One of an organization's key IT systems cannot be patched because the patches interfere with critical business application functionalities. Which of the following would be the risk practitioner's BEST recommendation?

- A. Additional mitigating controls should be identified.
- B. The system should not be used until the application is changed
- C. The organization's IT risk appetite should be adjusted.
- D. The associated IT risk should be accepted by management.

**Answer: A**

**NEW QUESTION 376**

- (Exam Topic 4)

Which of the following is the PRIMARY reason for an organization to include an acceptable use banner when users log in?

- A. To reduce the likelihood of insider threat
- B. To eliminate the possibility of insider threat
- C. To enable rapid discovery of insider threat
- D. To reduce the impact of insider threat

**Answer: A**

**NEW QUESTION 378**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 380**

- (Exam Topic 4)

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

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



D. Document the risk decision in the project risk register.

**Answer:** B

**NEW QUESTION 385**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 389**

- (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 391**

- (Exam Topic 4)

An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

- A. Identify the regulatory bodies that may highlight this gap
- B. Highlight news articles about data breaches
- C. Evaluate the risk as a measure of probable loss
- D. Verify if competitors comply with a similar policy

**Answer:** B

**NEW QUESTION 395**

- (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 398**

- (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 402**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 404**

- (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 406**

- (Exam Topic 4)

Who is MOST appropriate to be assigned ownership of a control

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

**Answer:** D

**NEW QUESTION 409**

- (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 411**

- (Exam Topic 4)

A risk practitioner observed Vial a high number of pokey exceptions were approved by senior management. Which of the following is the risk practitioner's BEST course of action to determine root cause?

- A. Review the risk profile
- B. Review pokey change history
- C. interview the control owner
- D. Perform control testing

**Answer:** C

**NEW QUESTION 414**

- (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 lime 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 416**

- (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 421**

- (Exam Topic 4)

Which of the following is MOST important for successful incident response?

- A. The quantity of data logged by the attack control tools
- B. Blocking the attack route immediately
- C. The ability to trace the source of the attack
- D. The timeliness of attack recognition

**Answer:** D

**NEW QUESTION 423**

- (Exam Topic 4)

Which of the following BEST reduces the risk associated with the theft of a laptop containing sensitive information?

- A. Cable lock
- B. Data encryption
- C. Periodic backup
- D. Biometrics access control

**Answer: B**

#### **NEW QUESTION 428**

- (Exam Topic 4)

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

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

**Answer: B**

#### **NEW QUESTION 429**

- (Exam Topic 4)

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

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

**Answer: C**

#### **NEW QUESTION 431**

- (Exam Topic 4)

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

- A. Marking the risk register available to project stakeholders
- B. Ensuring senior management commitment to risk training
- C. Providing regular communication to risk managers
- D. Appointing the risk manager from the business units

**Answer: B**

#### **NEW QUESTION 435**

- (Exam Topic 4)

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

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

**Answer: A**

#### **NEW QUESTION 437**

- (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 440**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 443**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 445**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 449**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 453**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 454**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 458**

- (Exam Topic 4)

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

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

**Answer: A**

**NEW QUESTION 463**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 465**

- (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 469**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 473**

- (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 478**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 479**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 482**

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 483

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 488

- (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 490

- (Exam Topic 3)

Which of the following BEST supports ethical IT risk management practices?

- A. Robust organizational communication channels
- B. Mapping of key risk indicators (KRIs) to corporate strategy
- C. Capability maturity models integrated with risk management frameworks
- D. Rigorously enforced operational service level agreements (SLAs)

**Answer:** A

#### NEW QUESTION 493

- (Exam Topic 3)

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

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

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

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

**Answer:** A

#### NEW QUESTION 495

- (Exam Topic 3)

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

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

**Answer:** B



**NEW QUESTION 498**

- (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 502**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 506**

- (Exam Topic 3)

What is the PRIMARY purpose of a business impact analysis (BIA)?

- A. To determine the likelihood and impact of threats to business operations
- B. To identify important business processes in the organization
- C. To estimate resource requirements for related business processes
- D. To evaluate the priority of business operations in case of disruption

**Answer: D**

**NEW QUESTION 509**

- (Exam Topic 3)

A risk practitioner has been asked by executives to explain how existing risk treatment plans would affect risk posture at the end of the year. Which of the following is MOST helpful in responding to this request?

- A. Assessing risk with no controls in place
- B. Showing projected residual risk
- C. Providing peer benchmarking results
- D. Assessing risk with current controls in place

**Answer: D**

**NEW QUESTION 512**

- (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 516**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 520**

- (Exam Topic 3)

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

- A. Obtain industry benchmarks related to the specific risk.
- B. Provide justification for the lower risk rating.
- C. Notify the business at the next risk briefing.



D. Reopen the risk issue and complete a full assessment.

**Answer:** B

**NEW QUESTION 525**

- (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 526**

- (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 529**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 533**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 537**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 540**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 542**

- (Exam Topic 3)

An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?

- A. Conduct a risk analysis.
- B. Initiate a remote data wipe.
- C. Invoke the incident response plan
- D. Disable the user account.

**Answer:** C

**NEW QUESTION 546**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 551**

- (Exam Topic 3)

Which of the following BEST indicates the effectiveness of anti-malware software?

- A. Number of staff hours lost due to malware attacks
- B. Number of downtime hours in business critical servers
- C. Number of patches made to anti-malware software
- D. Number of successful attacks by malicious software

**Answer:** D

**NEW QUESTION 555**

- (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 559**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 560**

- (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 564**

- (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 569**

- (Exam Topic 3)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery test of critical business processes?

- A. Percentage of job failures identified and resolved during the recovery process
- B. Percentage of processes recovered within the recovery time and point objectives
- C. Number of current test plans and procedures
- D. Number of issues and action items resolved during the recovery test

**Answer: B**

#### **NEW QUESTION 570**

- (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 574**

- (Exam Topic 3)

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

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

**Answer: C**

#### **NEW QUESTION 579**

- (Exam Topic 3)

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

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

**Answer: B**

#### **NEW QUESTION 583**

- (Exam Topic 3)

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

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

**Answer: B**

#### **NEW QUESTION 585**

- (Exam Topic 3)

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

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

**Answer: D**

#### **NEW QUESTION 587**

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 592

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 596

- (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 598

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 600

- (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 601

- (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 606

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 608

- (Exam Topic 3)

An organization practices the principle of least privilege. To ensure access remains appropriate, application owners should be required to review user access rights on a regular basis by obtaining:

- A. business purpose documentation and software license counts
- B. an access control matrix and approval from the user's manager

- C. documentation indicating the intended users of the application
- D. security logs to determine the cause of invalid login attempts

**Answer:** B

**NEW QUESTION 610**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 614**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 616**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 621**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 622**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 626**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 630**

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 635

- (Exam Topic 3)

Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?

- A. Piloting courses with focus groups
- B. Using reputable third-party training programs
- C. Reviewing content with senior management
- D. Creating modules for targeted audiences

**Answer:** D

#### NEW QUESTION 636

- (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 637

- (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 642

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 643

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 646

- (Exam Topic 2)

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

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



**Answer:** D

**NEW QUESTION 649**

- (Exam Topic 2)

The purpose of requiring source code escrow in a contractual agreement is to:

- A. ensure that the source code is valid and exists.
- B. ensure that the source code is available if the vendor ceases to exist.
- C. review the source code for adequacy of controls.
- D. ensure the source code is available when bugs occur.

**Answer:** B

**NEW QUESTION 652**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 653**

- (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 655**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 657**

- (Exam Topic 2)

Quantifying the value of a single asset helps the organization to understand the:

- A. overall effectiveness of risk management
- B. consequences of risk materializing
- C. necessity of developing a risk strategy,
- D. organization's risk threshold.

**Answer:** B

**NEW QUESTION 662**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 664**

- (Exam Topic 2)

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

- A. maximum tolerable downtime.
- B. maximum tolerable loss of data.



- C. need of each business unit.
- D. type of business.

**Answer:** C

**NEW QUESTION 669**

- (Exam Topic 2)

A risk practitioner has just learned about new done FIRST?

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

**Answer:** B

**NEW QUESTION 670**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 675**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 677**

- (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 679**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 681**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 682**

- (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 686**

- (Exam Topic 2)

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

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

**Answer:** A

#### **NEW QUESTION 688**

- (Exam Topic 2)

Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?

- A. Audit and compliance management
- B. The chief information officer (CIO) and the chief financial officer (CFO)
- C. Enterprise risk management and business process owners
- D. Executive management and the board of directors

**Answer:** D

#### **NEW QUESTION 690**

- (Exam Topic 2)

Who should be responsible for strategic decisions on risk management?

- A. Chief information officer (CIO)
- B. Executive management team
- C. Audit committee
- D. Business process owner

**Answer:** B

#### **NEW QUESTION 693**

- (Exam Topic 2)

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

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

**Answer:** B

#### **NEW QUESTION 694**

- (Exam Topic 2)

Which of the following is the BEST way to detect zero-day malware on an end user's workstation?

- A. An antivirus program
- B. Database activity monitoring
- C. Firewall log monitoring
- D. File integrity monitoring

**Answer:** C

#### **NEW QUESTION 698**

- (Exam Topic 2)

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

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

**Answer:** B

#### **NEW QUESTION 701**

- (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 702**

- (Exam Topic 2)

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

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

**Answer: A**

#### **NEW QUESTION 703**

- (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 705**

- (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 707**

- (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 710**

- (Exam Topic 2)

Deviation from a mitigation action plan's completion date should be determined by which of the following?

- A. Change management as determined by a change control board
- B. Benchmarking analysis with similar completed projects
- C. Project governance criteria as determined by the project office
- D. The risk owner as determined by risk management processes

**Answer: D**

#### **NEW QUESTION 711**

- (Exam Topic 2)

Which of the following is the MOST important information to be communicated during security awareness training?

- A. Management's expectations
- B. Corporate risk profile
- C. Recent security incidents
- D. The current risk management capability

**Answer: A**

#### NEW QUESTION 714

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 715

- (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 717

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 722

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 724

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 727

- (Exam Topic 2)

Which of the following will BEST help ensure that risk factors identified during an information systems review are addressed?

- A. Informing business process owners of the risk
- B. Reviewing and updating the risk register
- C. Assigning action items and deadlines to specific individuals
- D. Implementing new control technologies

**Answer: C**

#### NEW QUESTION 731

- (Exam Topic 2)

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

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

**Answer:**

B

**NEW QUESTION 735**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 740**

- (Exam Topic 2)

Which of the following is the GREATEST concern associated with business end users developing their own applications on end user spreadsheets and database programs?

- A. An IT project manager is not assigned to oversee development.
- B. Controls are not applied to the applications.
- C. There is a lack of technology recovery options.
- D. The applications are not captured in the risk profile.

**Answer: C**

**NEW QUESTION 744**

- (Exam Topic 2)

Which of the following is MOST likely to be impacted as a result of a new policy which allows staff members to remotely connect to the organization's IT systems via personal or public computers?

- A. Risk appetite
- B. Inherent risk
- C. Key risk indicator (KRI)
- D. Risk tolerance

**Answer: B**

**NEW QUESTION 749**

- (Exam Topic 2)

The MAIN purpose of a risk register is to:

- A. document the risk universe of the organization.
- B. promote an understanding of risk across the organization.
- C. enable well-informed risk management decisions.
- D. identify stakeholders associated with risk scenarios.

**Answer: C**

**NEW QUESTION 750**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 753**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 755**

- (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 759**

- (Exam Topic 2)

An IT risk practitioner is evaluating an organization's change management controls over the last six months. The GREATEST concern would be an increase in:

- A. rolled back changes below management's thresholds.
- B. change-related exceptions per month.
- C. the average implementation time for changes.
- D. number of user stories approved for implementation.

**Answer:** B

**NEW QUESTION 761**

- (Exam Topic 2)

Which of the following should an organization perform to forecast the effects of a disaster?

- A. Develop a business impact analysis (BIA).
- B. Define recovery time objectives (RTO).
- C. Analyze capability maturity model gaps.
- D. Simulate a disaster recovery.

**Answer:** A

**NEW QUESTION 764**

- (Exam Topic 2)

Which of the following is the FIRST step when developing a business case to drive the adoption of a risk remediation project by senior management?

- A. Calculating the cost
- B. Analyzing cost-effectiveness
- C. Determining the stakeholders
- D. Identifying the objectives

**Answer:** A

**NEW QUESTION 767**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 772**

- (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 773**

- (Exam Topic 2)

Which of the following is the GREATEST concern when using a generic set of IT risk scenarios for risk analysis?

- A. Quantitative analysis might not be possible.
- B. Risk factors might not be relevant to the organization
- C. Implementation costs might increase.
- D. Inherent risk might not be considered.

**Answer:** B

**NEW QUESTION 776**

- (Exam Topic 2)



Which of the following is the MOST effective way to mitigate identified risk scenarios?

- A. Assign ownership of the risk response plan
- B. Provide awareness in early detection of risk.
- C. Perform periodic audits on identified risk.
- D. areas Document the risk tolerance of the organization.

**Answer:** A

#### **NEW QUESTION 778**

- (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 781**

- (Exam Topic 2)

Mitigating technology risk to acceptable levels should be based PRIMARILY upon:

- A. organizational risk appetite.
- B. business sector best practices.
- C. business process requirements.
- D. availability of automated solutions

**Answer:** C

#### **NEW QUESTION 785**

- (Exam Topic 2)

An organization has outsourced a critical process involving highly regulated data to a third party with servers located in a foreign country. Who is accountable for the confidentiality of this data?

- A. Third-party data custodian
- B. Data custodian
- C. Regional office executive
- D. Data owner

**Answer:** D

#### **NEW QUESTION 788**

- (Exam Topic 2)

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

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

**Answer:** B

#### **NEW QUESTION 789**

- (Exam Topic 2)

Which of the following should management consider when selecting a risk mitigation option?

- A. Maturity of the enterprise architecture
- B. Cost of control implementation
- C. Reliability of key performance indicators (KPIs)
- D. Reliability of key risk indicators (KRIs)

**Answer:** B

#### **NEW QUESTION 794**

- (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 797

- (Exam Topic 2)

Which of the following BEST supports the communication of risk assessment results to stakeholders?

- A. Monitoring of high-risk areas
- B. Classification of risk profiles
- C. Periodic review of the risk register
- D. Assignment of risk ownership

**Answer: D**

#### NEW QUESTION 798

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 802

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 805

- (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 810

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 812

- (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 813

- (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 815**

- (Exam Topic 2)

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

- A. Key performance indicators
- B. Business objectives
- C. The organization's risk framework
- D. Risk appetite

**Answer:** B

**NEW QUESTION 820**

- (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 822**

- (Exam Topic 2)

Which of the following is the BEST way to determine software license compliance?

- A. List non-compliant systems in the risk register.
- B. Conduct periodic compliance reviews.
- C. Review whistleblower reports of noncompliance.
- D. Monitor user software download activity.

**Answer:** B

**NEW QUESTION 823**

- (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 827**

- (Exam Topic 2)

Which of the following is MOST helpful in identifying gaps between the current and desired state of the IT risk environment?

- A. Analyzing risk appetite and tolerance levels
- B. Assessing identified risk and recording results in the risk register
- C. Evaluating risk scenarios and assessing current controls
- D. Reviewing guidance from industry best practices and standards

**Answer:** C

**NEW QUESTION 829**

- (Exam Topic 2)

Which of the following would MOST likely result in updates to an IT risk appetite statement?

- A. External audit findings
- B. Feedback from focus groups
- C. Self-assessment reports
- D. Changes in senior management

**Answer:** D

**NEW QUESTION 832**

- (Exam Topic 2)

Which of The following would offer the MOST insight with regard to an organization's risk culture?

- A. Risk management procedures
- B. Senior management interviews
- C. Benchmark analyses

D. Risk management framework

**Answer:** B

**NEW QUESTION 833**

- (Exam Topic 2)

Which of the following risk register elements is MOST likely to be updated if the attack surface or exposure of an asset is reduced?

- A. Likelihood rating
- B. Control effectiveness
- C. Assessment approach
- D. Impact rating

**Answer:** A

**NEW QUESTION 836**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 839**

- (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 840**

- (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 844**

- (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 846**

- (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 848**

- (Exam Topic 2)

A control owner has completed a year-long project To strengthen existing controls. It is MOST important for the risk practitioner to:

- A. update the risk register to reflect the correct level of residual risk.
- B. ensure risk monitoring for the project is initiated.
- C. conduct and document a business impact analysis (BIA).
- D. verify cost-benefit of the new controls being implemented.

**Answer:** A

**NEW QUESTION 851**

- (Exam Topic 2)

A risk practitioner observes that the fraud detection controls in an online payment system do not perform as expected. Which of the following will MOST likely change as a result?

- A. Impact
- B. Residual risk
- C. Inherent risk
- D. Risk appetite

**Answer:** B

**NEW QUESTION 852**

- (Exam Topic 2)

Which of the following would provide the MOST comprehensive information for updating an organization's risk register?

- A. Results of the latest risk assessment
- B. Results of a risk forecasting analysis
- C. A review of compliance regulations
- D. Findings of the most recent audit

**Answer:** A

**NEW QUESTION 857**

.....

## 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](#)**