

# Isaca

## Exam Questions CRISC

Certified in Risk and Information Systems Control



**NEW QUESTION 1**

- (Exam Topic 1)

From a business perspective, which of the following is the MOST important objective of a disaster recovery test?

- A. The organization gains assurance it can recover from a disaster
- B. Errors are discovered in the disaster recovery process.
- C. All business critical systems are successfully tested.
- D. All critical data is recovered within recovery time objectives (RTOs).

**Answer: B**

**NEW QUESTION 2**

- (Exam Topic 1)

What is the BEST information to present to business control owners when justifying costs related to controls?

- A. Loss event frequency and magnitude
- B. The previous year's budget and actuals
- C. Industry benchmarks and standards
- D. Return on IT security-related investments

**Answer: D**

**NEW QUESTION 3**

- (Exam Topic 1)

When using a third party to perform penetration testing, which of the following is the MOST important control to minimize operational impact?

- A. Perform a background check on the vendor.
- B. Require the vendor to sign a nondisclosure agreement.
- C. Require the vendor to have liability insurance.
- D. Clearly define the project scope

**Answer: D**

**NEW QUESTION 4**

- (Exam Topic 1)

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:

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: B**

**NEW QUESTION 5**

- (Exam Topic 1)

The acceptance of control costs that exceed risk exposure is MOST likely an example of:

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

**Answer: B**

**NEW QUESTION 6**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 7**

- (Exam Topic 1)

Which of the following will BEST help mitigate the risk associated with malicious functionality in outsourced application development?

- A. Perform an m-depth code review with an expert
- B. Validate functionality by running in a test environment
- C. Implement a service level agreement.
- D. Utilize the change management process.

**Answer:** C

**NEW QUESTION 8**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 9**

- (Exam Topic 1)

An organization delegates its data processing to the internal IT team to manage information through its applications. Which of the following is the role of the internal IT team in this situation?

- A. Data controllers
- B. Data processors
- C. Data custodians
- D. Data owners

**Answer:** B

**NEW QUESTION 10**

- (Exam Topic 1)

Which of the following is the BEST indication of an improved risk-aware culture following the implementation of a security awareness training program for all employees?

- A. A reduction in the number of help desk calls
- B. An increase in the number of identified system flaws
- C. A reduction in the number of user access resets
- D. An increase in the number of incidents reported

**Answer:** B

**NEW QUESTION 10**

- (Exam Topic 1)

Which of the following is of GREATEST concern when uncontrolled changes are made to the control environment?

- A. A decrease in control layering effectiveness
- B. An increase in inherent risk
- C. An increase in control vulnerabilities
- D. An increase in the level of residual risk

**Answer:** D

**NEW QUESTION 15**

- (Exam Topic 1)

Which of the following is the MAIN reason to continuously monitor IT-related risk?

- A. To redefine the risk appetite and risk tolerance levels based on changes in risk factors
- B. To update the risk register to reflect changes in levels of identified and new IT-related risk
- C. To ensure risk levels are within acceptable limits of the organization's risk appetite and risk tolerance
- D. To help identify root causes of incidents and recommend suitable long-term solutions

**Answer:** C

**NEW QUESTION 16**

- (Exam Topic 1)

Which of the following is the MOST important element of a successful risk awareness training program?

- A. Customizing content for the audience

- B. Providing incentives to participants
- C. Mapping to a recognized standard
- D. Providing metrics for measurement

**Answer:** A

**NEW QUESTION 21**

- (Exam Topic 1)

Which of the following should be the PRIMARY objective of promoting a risk-aware culture within an organization?

- A. Better understanding of the risk appetite
- B. Improving audit results
- C. Enabling risk-based decision making
- D. Increasing process control efficiencies

**Answer:** C

**NEW QUESTION 24**

- (Exam Topic 1)

Calculation of the recovery time objective (RTO) is necessary to determine the:

- A. time required to restore files.
- B. point of synchronization
- C. priority of restoration.
- D. annual loss expectancy (ALE).

**Answer:** A

**NEW QUESTION 26**

- (Exam Topic 1)

Which of the following is the BEST metric to demonstrate the effectiveness of an organization's change management process?

- A. Increase in the frequency of changes
- B. Percent of unauthorized changes
- C. Increase in the number of emergency changes
- D. Average time to complete changes

**Answer:** B

**NEW QUESTION 29**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 34**

- (Exam Topic 1)

Which of the following is the BEST key performance indicator (KPI) to measure the maturity of an organization's security incident handling process?

- A. The number of security incidents escalated to senior management
- B. The number of resolved security incidents
- C. The number of newly identified security incidents
- D. The number of recurring security incidents

**Answer:** B

**NEW QUESTION 36**

- (Exam Topic 1)

Which of the following is MOST important to understand when determining an appropriate risk assessment approach?

- A. Complexity of the IT infrastructure
- B. Value of information assets
- C. Management culture
- D. Threats and vulnerabilities

**Answer:** A

**NEW QUESTION 39**

- (Exam Topic 1)

Which of the following risk register updates is MOST important for senior management to review?

- A. Extending the date of a future action plan by two months
- B. Retiring a risk scenario no longer used
- C. Avoiding a risk that was previously accepted
- D. Changing a risk owner

**Answer:** A

**NEW QUESTION 43**

- (Exam Topic 1)

Which of the following provides the BEST evidence of the effectiveness of an organization's account provisioning process?

- A. User provisioning
- B. Role-based access controls
- C. Security log monitoring
- D. Entitlement reviews

**Answer:** B

**NEW QUESTION 47**

- (Exam Topic 1)

Which of the following is the GREATEST benefit of incorporating IT risk scenarios into the corporate risk register?

- A. Corporate incident escalation protocols are established.
- B. Exposure is integrated into the organization's risk profile.
- C. Risk appetite cascades to business unit management
- D. The organization-wide control budget is expanded.

**Answer:** B

**NEW QUESTION 52**

- (Exam Topic 1)

Which of the following is the MAIN reason for documenting the performance of controls?

- A. Obtaining management sign-off
- B. Demonstrating effective risk mitigation
- C. Justifying return on investment
- D. Providing accurate risk reporting

**Answer:** D

**NEW QUESTION 57**

- (Exam Topic 1)

Which of the following attributes of a key risk indicator (KRI) is MOST important?

- A. Repeatable
- B. Automated
- C. Quantitative
- D. Qualitative

**Answer:** A

**NEW QUESTION 60**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 64**

- (Exam Topic 1)

Which of the following is the MOST critical element to maximize the potential for a successful security implementation?

- A. The organization's knowledge
- B. Ease of implementation
- C. The organization's culture
- D. industry-leading security tools

**Answer:** C

**NEW QUESTION 65**

- (Exam Topic 1)

After a risk has been identified, who is in the BEST position to select the appropriate risk treatment option?

- A. The risk practitioner
- B. The business process owner
- C. The risk owner
- D. The control owner

**Answer:** C

#### **NEW QUESTION 69**

- (Exam Topic 1)

In an organization with a mature risk management program, which of the following would provide the BEST evidence that the IT risk profile is up to date?

- A. Risk questionnaire
- B. Risk register
- C. Management assertion
- D. Compliance manual

**Answer:** B

#### **NEW QUESTION 73**

- (Exam Topic 1)

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

- A. Key risk indicators
- B. Risk scenarios
- C. Business impact analysis
- D. Threat analysis

**Answer:** B

#### **NEW QUESTION 77**

- (Exam Topic 1)

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

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

**Answer:** A

#### **NEW QUESTION 81**

- (Exam Topic 1)

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 85**

- (Exam Topic 1)

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

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

**Answer:** C

#### **NEW QUESTION 89**

- (Exam Topic 1)

Which of the following is MOST helpful in identifying new risk exposures due to changes in the business environment?

- A. Standard operating procedures
- B. SWOT analysis
- C. Industry benchmarking
- D. Control gap analysis

**Answer:** B

#### **NEW QUESTION 91**

- (Exam Topic 1)

A data processing center operates in a jurisdiction where new regulations have significantly increased penalties for data breaches. Which of the following elements of the risk register is MOST important to update to reflect this change?

- A. Risk impact
- B. Risk trend
- C. Risk appetite
- D. Risk likelihood

**Answer:** A

#### NEW QUESTION 95

- (Exam Topic 1)

Which of the following elements of a risk register is MOST likely to change as a result of change in management's risk appetite?

- A. Key risk indicator (KRI) thresholds
- B. Inherent risk
- C. Risk likelihood and impact
- D. Risk velocity

**Answer:** A

#### NEW QUESTION 98

- (Exam Topic 1)

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

- A. Assisting in continually optimizing risk governance
- B. Enabling the documentation and analysis of trends
- C. Ensuring compliance with regulatory requirements
- D. Providing an early warning to take proactive actions

**Answer:** D

#### NEW QUESTION 100

- (Exam Topic 1)

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 103

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 107

- (Exam Topic 1)

The MAIN purpose of conducting a control self-assessment (CSA) is to:

- A. gain a better understanding of the control effectiveness in the organization
- B. gain a better understanding of the risk in the organization
- C. adjust the controls prior to an external audit
- D. reduce the dependency on external audits

**Answer:** A

#### NEW QUESTION 109

- (Exam Topic 1)

An unauthorized individual has socially engineered entry into an organization's secured physical premises. Which of the following is the BEST way to prevent future occurrences?

- A. Employ security guards.
- B. Conduct security awareness training.
- C. Install security cameras.
- D. Require security access badges.

**Answer:** B



#### NEW QUESTION 110

- (Exam Topic 1)

Which of the following roles would provide the MOST important input when identifying IT risk scenarios?

- A. Information security managers
- B. Internal auditors
- C. Business process owners
- D. Operational risk managers

**Answer: C**

#### NEW QUESTION 111

- (Exam Topic 1)

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

- A. Emerging risk must be continuously reported to management.
- B. New system vulnerabilities emerge at frequent intervals.
- C. The risk environment is subject to change.
- D. The information security budget must be justified.

**Answer: C**

#### NEW QUESTION 113

- (Exam Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 117

- (Exam Topic 1)

Which of the following would be MOST important for a risk practitioner to provide to the internal audit department during the audit planning process?

- A. Closed management action plans from the previous audit
- B. Annual risk assessment results
- C. An updated vulnerability management report
- D. A list of identified generic risk scenarios

**Answer: A**

#### NEW QUESTION 122

- (Exam Topic 1)

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 124

- (Exam Topic 1)

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: A**

#### NEW QUESTION 127

- (Exam Topic 1)

Which of the following would be the BEST way to help ensure the effectiveness of a data loss prevention (DLP) control that has been implemented to prevent the loss of credit card data?

- A. Testing the transmission of credit card numbers
- B. Reviewing logs for unauthorized data transfers



- C. Configuring the DLP control to block credit card numbers
- D. Testing the DLP rule change control process

**Answer:** A

**NEW QUESTION 131**

- (Exam Topic 1)

The BEST reason to classify IT assets during a risk assessment is to determine the:

- A. priority in the risk register.
- B. business process owner.
- C. enterprise risk profile.
- D. appropriate level of protection.

**Answer:** D

**NEW QUESTION 136**

- (Exam Topic 1)

It is MOST appropriate for changes to be promoted to production after they are;

- A. communicated to business management
- B. tested by business owners.
- C. approved by the business owner.
- D. initiated by business users.

**Answer:** B

**NEW QUESTION 140**

- (Exam Topic 1)

An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?

- A. Perform a risk assessment
- B. Disable user access.
- C. Develop an access control policy.
- D. Perform root cause analysis.

**Answer:** B

**NEW QUESTION 143**

- (Exam Topic 1)

A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application. Who should have the authority to accept the associated risk?

- A. Business continuity director
- B. Disaster recovery manager
- C. Business application owner
- D. Data center manager

**Answer:** C

**NEW QUESTION 148**

- (Exam Topic 1)

Which of the following aspects of an IT risk and control self-assessment would be MOST important to include in a report to senior management?

- A. Changes in control design
- B. A decrease in the number of key controls
- C. Changes in control ownership
- D. An increase in residual risk

**Answer:** D

**NEW QUESTION 153**

- (Exam Topic 1)

Which of the following is a PRIMARY benefit of engaging the risk owner during the risk assessment process?

- A. Identification of controls gaps that may lead to noncompliance
- B. Prioritization of risk action plans across departments
- C. Early detection of emerging threats
- D. Accurate measurement of loss impact

**Answer:** D

**NEW QUESTION 155**

- (Exam Topic 1)

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 159**

- (Exam Topic 1)

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 164**

- (Exam Topic 1)

Which of the following is the MOST important foundational element of an effective three lines of defense model for an organization?

- A. A robust risk aggregation tool set
- B. Clearly defined roles and responsibilities
- C. A well-established risk management committee
- D. Well-documented and communicated escalation procedures

**Answer:** B

**NEW QUESTION 168**

- (Exam Topic 1)

Which of the following would BEST help minimize the risk associated with social engineering threats?

- A. Enforcing employees sanctions
- B. Conducting phishing exercises
- C. Enforcing segregation of duties
- D. Reviewing the organization's risk appetite

**Answer:** B

**NEW QUESTION 169**

- (Exam Topic 1)

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 174**

- (Exam Topic 1)

Which of the following would be MOST useful when measuring the progress of a risk response action plan?

- A. Percentage of mitigated risk scenarios
- B. Annual loss expectancy (ALE) changes
- C. Resource expenditure against budget
- D. An up-to-date risk register

**Answer:** D

**NEW QUESTION 179**

- (Exam Topic 1)

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:** A

**NEW QUESTION 180**

- (Exam Topic 1)

Which of the following activities would BEST contribute to promoting an organization-wide risk-aware culture?

- A. Performing a benchmark analysis and evaluating gaps
- B. Conducting risk assessments and implementing controls
- C. Communicating components of risk and their acceptable levels
- D. Participating in peer reviews and implementing best practices

**Answer: C**

#### NEW QUESTION 184

- (Exam Topic 1)

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: B**

#### NEW QUESTION 185

- (Exam Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 190

- (Exam Topic 1)

After undertaking a risk assessment of a production system, the MOST appropriate action is for the risk manager to:

- A. recommend a program that minimizes the concerns of that production system.
- B. inform the development team of the concerns, and together formulate risk reduction measures.
- C. inform the process owner of the concerns and propose measures to reduce them
- D. inform the IT manager of the concerns and propose measures to reduce them.

**Answer: A**

#### NEW QUESTION 193

- (Exam Topic 1)

Which of the following is the MOST important factor affecting risk management in an organization?

- A. The risk manager's expertise
- B. Regulatory requirements
- C. Board of directors' expertise
- D. The organization's culture

**Answer: B**

#### NEW QUESTION 195

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 196

- (Exam Topic 1)

A review of an organization's controls has determined its data loss prevention (DLP) system is currently failing to detect outgoing emails containing credit card data. Which of the following would be MOST impacted?

- A. Key risk indicators (KRIs)
- B. Inherent risk
- C. Residual risk
- D. Risk appetite

**Answer: C**

#### NEW QUESTION 198

- (Exam Topic 2)

Which of the following would present the GREATEST challenge when assigning accountability for control ownership?

- A. Weak governance structures
- B. Senior management scrutiny
- C. Complex regulatory environment
- D. Unclear reporting relationships

**Answer: D**

#### NEW QUESTION 199

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 204

- (Exam Topic 2)

A maturity model will BEST indicate:

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

**Answer: B**

#### NEW QUESTION 208

- (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: A**

#### NEW QUESTION 209

- (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: D**

#### NEW QUESTION 210

- (Exam Topic 2)

Which of the following should be of GREATEST concern to a risk practitioner when determining the effectiveness of IT controls?

- A. Configuration updates do not follow formal change control.
- B. Operational staff perform control self-assessments.
- C. Controls are selected without a formal cost-benefit
- D. analysis-Management reviews security policies once every two years.

**Answer: A**

#### NEW QUESTION 215

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 219**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 223**

- (Exam Topic 2)

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 228**

- (Exam Topic 2)

Which of the following should be the MOST important consideration when performing a vendor risk assessment?

- A. Results of the last risk assessment of the vendor
- B. Inherent risk of the business process supported by the vendor
- C. Risk tolerance of the vendor
- D. Length of time since the last risk assessment of the vendor

**Answer:** B

**NEW QUESTION 230**

- (Exam Topic 2)

Which of the following is MOST helpful in aligning IT risk with business objectives?

- A. Introducing an approved IT governance framework
- B. Integrating the results of top-down risk scenario analyses
- C. Performing a business impact analysis (BIA)
- D. Implementing a risk classification system

**Answer:** A

**NEW QUESTION 232**

- (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:** D

**NEW QUESTION 234**

- (Exam Topic 2)

An organization has decided to implement an emerging technology and incorporate the new capabilities into its strategic business plan. Business operations for the technology will be outsourced. What will be the risk practitioner's PRIMARY role during the change?

- A. Managing third-party risk
- B. Developing risk scenarios
- C. Managing the threat landscape
- D. Updating risk appetite

**Answer:** B

**NEW QUESTION 236**

- (Exam Topic 2)

A new policy has been published to forbid copying of data onto removable media. Which type of control has been implemented?

- A. Preventive
- B. Detective
- C. Directive
- D. Deterrent

**Answer: C**

**NEW QUESTION 241**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 243**

- (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 244**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 246**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 251**

- (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 254**

- (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 258**



- (Exam Topic 2)

Which of the following BEST promotes commitment to controls?

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

**Answer:** A

#### NEW QUESTION 260

- (Exam Topic 2)

Which of the following is a detective control?

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

**Answer:** B

#### NEW QUESTION 265

- (Exam Topic 2)

Which of the following would be MOST relevant to stakeholders regarding ineffective control implementation?

- A. Threat to IT
- B. Number of control failures
- C. Impact on business
- D. Risk ownership

**Answer:** C

#### NEW QUESTION 269

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 273

- (Exam Topic 2)

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 275

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 276

- (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 278**

- (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:** D

**NEW QUESTION 280**

- (Exam Topic 2)

When updating a risk register with the results of an IT risk assessment, the risk practitioner should log:

- A. high impact scenarios.
- B. high likelihood scenarios.
- C. treated risk scenarios.
- D. known risk scenarios.

**Answer:** D

**NEW QUESTION 282**

- (Exam Topic 2)

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 283**

- (Exam Topic 2)

A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (PII). Which of the following will MOST likely outcome for an organization affected by the new law?

- A. Increase in compliance breaches
- B. Increase in loss event impact
- C. Increase in residual risk
- D. Increase in customer complaints

**Answer:** B

**NEW QUESTION 286**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 290**

- (Exam Topic 2)

An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

- A. Review the risk identification process.
- B. Inform the risk scenario owners.
- C. Create a risk awareness communication plan.
- D. Update the risk register.

**Answer:** A

**NEW QUESTION 295**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 298**

- (Exam Topic 2)

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 301**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 304**

- (Exam Topic 2)

An organization has decided to outsource a web application, and customer data will be stored in the vendor's public cloud. To protect customer data, it is MOST important to ensure which of the following?

- A. The organization's incident response procedures have been updated.
- B. The vendor stores the data in the same jurisdiction.
- C. Administrative access is only held by the vendor.
- D. The vendor's responsibilities are defined in the contract.

**Answer:** D

**NEW QUESTION 307**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 310**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 313**

- (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:** B

**NEW QUESTION 315**

- (Exam Topic 2)

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 319**

- (Exam Topic 2)

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

- A. Balanced scorecard
- B. Risk register
- C. Business impact analysis
- D. Heat map

**Answer:** D

**NEW QUESTION 320**

- (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 321**

- (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 323**

- (Exam Topic 2)

Which of the following will BEST help an organization select a recovery strategy for critical systems?

- A. Review the business impact analysis.
- B. Create a business continuity plan.
- C. Analyze previous disaster recovery reports.
- D. Conduct a root cause analysis.

**Answer:** A

**NEW QUESTION 327**

- (Exam Topic 2)

When reporting on the performance of an organization's control environment including which of the following would BEST inform stakeholders risk decision-making?

- A. The audit plan for the upcoming period
- B. Spend to date on mitigating control implementation
- C. A report of deficiencies noted during controls testing
- D. A status report of control deployment

**Answer:** C

**NEW QUESTION 329**

- (Exam Topic 2)

Which of the following BEST indicates effective information security incident management?

- A. Monthly trend of information security-related incidents
- B. Average time to identify critical information security incidents
- C. Frequency of information security incident response plan testing
- D. Percentage of high risk security incidents

**Answer:** B

**NEW QUESTION 330**

- (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 betng implemented.

**Answer:** A

#### **NEW QUESTION 334**

- (Exam Topic 2)

An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?

- A. Implement IT systems in alignment with business objectives.
- B. Review metrics and key performance indicators (KPIs).
- C. Review design documentation of IT systems.
- D. Evaluate compliance with legal and regulatory requirements.

**Answer:** B

#### **NEW QUESTION 339**

- (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 342**

- (Exam Topic 2)

The MOST important reason to aggregate results from multiple risk assessments on interdependent information systems is to:

- A. establish overall impact to the organization
- B. efficiently manage the scope of the assignment
- C. identify critical information systems
- D. facilitate communication to senior management

**Answer:** A

#### **NEW QUESTION 346**

.....

## 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](#)**