

# Isaca

## Exam Questions CRISC

Certified in Risk and Information Systems Control



#### NEW QUESTION 1

- (Exam Topic 1)

Which of the following is the BEST course of action to reduce risk impact?

- A. Create an IT security policy.
- B. Implement corrective measures.
- C. Implement detective controls.
- D. Leverage existing technology

**Answer: B**

#### NEW QUESTION 2

- (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 3

- (Exam Topic 1)

The PRIMARY objective of testing the effectiveness of a new control before implementation is to:

- A. ensure that risk is mitigated by the control.
- B. measure efficiency of the control process.
- C. confirm control alignment with business objectives.
- D. comply with the organization's policy.

**Answer: C**

#### NEW QUESTION 4

- (Exam Topic 1)

In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

- A. Establishing an intellectual property agreement
- B. Evaluating each of the data sources for vulnerabilities
- C. Periodically reviewing big data strategies
- D. Benchmarking to industry best practice

**Answer: C**

#### NEW QUESTION 5

- (Exam Topic 1)

Which of the following would be a risk practitioners BEST recommendation for preventing cyber intrusion?

- A. Establish a cyber response plan
- B. Implement data loss prevention (DLP) tools.
- C. Implement network segregation.
- D. Strengthen vulnerability remediation efforts.

**Answer: D**

#### NEW QUESTION 6

- (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 7**

- (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 8**

- (Exam Topic 1)

Which of the following is the MOST cost-effective way to test a business continuity plan?

- A. Conduct interviews with key stakeholders.
- B. Conduct a tabletop exercise.
- C. Conduct a disaster recovery exercise.
- D. Conduct a full functional exercise.

**Answer:** B

**NEW QUESTION 9**

- (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 10**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 10**

- (Exam Topic 1)

The head of a business operations department asks to review the entire IT risk register. Which of the following would be the risk manager s BEST approach to this request before sharing the register?

- A. Escalate to senior management
- B. Require a nondisclosure agreement.
- C. Sanitize portions of the register
- D. Determine the purpose of the request

**Answer:** D

**NEW QUESTION 14**

- (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 19**

- (Exam Topic 1)

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 20**

- (Exam Topic 1)

The analysis of which of the following will BEST help validate whether suspicious network activity is malicious?

- A. Logs and system events
- B. Intrusion detection system (IDS) rules
- C. Vulnerability assessment reports
- D. Penetration test reports

**Answer:** B

**NEW QUESTION 25**

- (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 29**

- (Exam Topic 1)

The MOST important characteristic of an organization's policies is to reflect the organization's:

- A. risk assessment methodology.
- B. risk appetite.
- C. capabilities
- D. asset value.

**Answer:** B

**NEW QUESTION 30**

- (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 33**

- (Exam Topic 1)

IT risk assessments can BEST be used by management:

- A. for compliance with laws and regulations
- B. as a basis for cost-benefit analysis.
- C. as input for decision-making
- D. to measure organizational success.

**Answer:** C

**NEW QUESTION 36**

- (Exam Topic 1)

A trusted third party service provider has determined that the risk of a client's systems being hacked is low. Which of the following would be the client's BEST course of action?

- A. Perform their own risk assessment
- B. Implement additional controls to address the risk.
- C. Accept the risk based on the third party's risk assessment
- D. Perform an independent audit of the third party.

**Answer:** C

**NEW QUESTION 40**

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 41

- (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 43

- (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 44

- (Exam Topic 1)

An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?

- A. Invoke the disaster recovery plan during an incident.
- B. Prepare a cost-benefit analysis of alternatives available
- C. Implement redundant infrastructure for the application.
- D. Reduce the recovery time by strengthening the response team.

**Answer: C**

#### NEW QUESTION 47

- (Exam Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 50

- (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 51

- (Exam Topic 1)

Which of the following is MOST important when developing key performance indicators (KPIs)?

- A. Alignment to risk responses
- B. Alignment to management reports
- C. Alerts when risk thresholds are reached
- D. Identification of trends

**Answer: C**

**NEW QUESTION 56**

- (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 57**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 62**

- (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 65**

- (Exam Topic 1)

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

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

**Answer:** D

**NEW QUESTION 68**

- (Exam Topic 1)

A risk practitioner is organizing risk awareness training for senior management. Which of the following is the MOST important topic to cover in the training session?

- A. The organization's strategic risk management projects
- B. Senior management roles and responsibilities
- C. The organizations risk appetite and tolerance
- D. Senior management allocation of risk management resources

**Answer:** B

**NEW QUESTION 69**

- (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 74**

- (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 75**

- (Exam Topic 1)

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 78**

- (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 81**

- (Exam Topic 1)

During testing, a risk practitioner finds the IT department's recovery time objective (RTO) for a key system does not align with the enterprise's business continuity plan (BCP). Which of the following should be done NEXT?

- A. Report the gap to senior management
- B. Consult with the IT department to update the RTO
- C. Complete a risk exception form.
- D. Consult with the business owner to update the BCP

**Answer:** A

**NEW QUESTION 84**

- (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 86**

- (Exam Topic 1)

Which of the following is MOST useful when communicating risk to management?

- A. Risk policy
- B. Audit report
- C. Risk map
- D. Maturity model

**Answer:** A

**NEW QUESTION 91**

- (Exam Topic 1)

Which of the following IT controls is MOST useful in mitigating the risk associated with inaccurate data?

- A. Encrypted storage of data
- B. Links to source data
- C. Audit trails for updates and deletions
- D. Check totals on data records and data fields

**Answer:** C

**NEW QUESTION 93**

- (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 95**

- (Exam Topic 1)

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 97**

- (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 102**

- (Exam Topic 1)

Which of the following should be the PRIMARY input when designing IT controls?

- A. Benchmark of industry standards
- B. Internal and external risk reports
- C. Recommendations from IT risk experts
- D. Outcome of control self-assessments

**Answer:** B

**NEW QUESTION 107**

- (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 108**

- (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 111**

- (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 114**

- (Exam Topic 1)

Which of the following would be- MOST helpful to understand the impact of a new technology system on an organization's current risk profile?



- A. Hire consultants specializing in the new technology.
- B. Review existing risk mitigation controls.
- C. Conduct a gap analysis.
- D. Perform a risk assessment.

**Answer: D**

**NEW QUESTION 119**

- (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 124**

- (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 128**

- (Exam Topic 1)

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

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

**Answer: B**

**NEW QUESTION 132**

- (Exam Topic 1)

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: A**

**NEW QUESTION 136**

- (Exam Topic 1)

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

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

**Answer: A**

**NEW QUESTION 141**

- (Exam Topic 1)

To implement the MOST effective monitoring of key risk indicators (KRIs), which of the following needs to be in place?

- A. Threshold definition
- B. Escalation procedures
- C. Automated data feed
- D. Controls monitoring

**Answer: A**

**NEW QUESTION 143**

- (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 144**

- (Exam Topic 1)

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

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

**Answer:** B

#### **NEW QUESTION 148**

- (Exam Topic 1)

Which of the following would BEST help to ensure that identified risk is efficiently managed?

- A. Reviewing the maturity of the control environment
- B. Regularly monitoring the project plan
- C. Maintaining a key risk indicator for each asset in the risk register
- D. Periodically reviewing controls per the risk treatment plan

**Answer:** D

#### **NEW QUESTION 150**

- (Exam Topic 1)

During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall. Which of the following controls has MOST likely been compromised?

- A. Data validation
- B. Identification
- C. Authentication
- D. Data integrity

**Answer:** C

#### **NEW QUESTION 153**

- (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 158**

- (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 163**

- (Exam Topic 1)

Which of the following would provide the BEST guidance when selecting an appropriate risk treatment plan?

- A. Risk mitigation budget
- B. Business Impact analysis
- C. Cost-benefit analysis
- D. Return on investment

**Answer:** B

**NEW QUESTION 167**

- (Exam Topic 1)

A business unit is updating a risk register with assessment results for a key project. Which of the following is MOST important to capture in the register?

- A. The team that performed the risk assessment
- B. An assigned risk manager to provide oversight
- C. Action plans to address risk scenarios requiring treatment
- D. The methodology used to perform the risk assessment

**Answer: B**

**NEW QUESTION 168**

- (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 172**

- (Exam Topic 1)

Which of the following issues should be of GREATEST concern when evaluating existing controls during a risk assessment?

- A. A high number of approved exceptions exist with compensating controls.
- B. Successive assessments have the same recurring vulnerabilities.
- C. Redundant compensating controls are in place.
- D. Asset custodians are responsible for defining controls instead of asset owners.

**Answer: D**

**NEW QUESTION 177**

- (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 179**

- (Exam Topic 1)

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

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

**Answer: C**

**NEW QUESTION 183**

- (Exam Topic 1)

Which of the following is the BEST way to determine the ongoing efficiency of control processes?

- A. Perform annual risk assessments.
- B. Interview process owners.
- C. Review the risk register.
- D. Analyze key performance indicators (KPIs).

**Answer: D**

**NEW QUESTION 184**

- (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 186**

- (Exam Topic 1)

Which of the following would BEST help to ensure that suspicious network activity is identified?

- A. Analyzing intrusion detection system (IDS) logs
- B. Analyzing server logs
- C. Using a third-party monitoring provider
- D. Coordinating events with appropriate agencies

**Answer:** A

**NEW QUESTION 190**

- (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 191**

- (Exam Topic 1)

Which of the following is MOST critical when designing controls?

- A. Involvement of internal audit
- B. Involvement of process owner
- C. Quantitative impact of the risk
- D. Identification of key risk indicators

**Answer:** B

**NEW QUESTION 195**

- (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 200**

- (Exam Topic 1)

Which of the following should be the PRIMARY consideration when implementing controls for monitoring user activity logs?

- A. Ensuring availability of resources for log analysis
- B. Implementing log analysis tools to automate controls
- C. Ensuring the control is proportional to the risk
- D. Building correlations between logs collected from different sources

**Answer:** C

**NEW QUESTION 202**

- (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 206**

- (Exam Topic 1)

An effective control environment is BEST indicated by controls that:

- A. minimize senior management's risk tolerance.
- B. manage risk within the organization's risk appetite.
- C. reduce the thresholds of key risk indicators (KRIs).
- D. are cost-effective to implement

**Answer:** B

**NEW QUESTION 210**

- (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 214**

- (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 218**

- (Exam Topic 1)

When determining which control deficiencies are most significant, which of the following would provide the MOST useful information?

- A. Risk analysis results
- B. Exception handling policy
- C. Vulnerability assessment results
- D. Benchmarking assessments

**Answer:** C

**NEW QUESTION 223**

- (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 225**

- (Exam Topic 1)

Management has noticed storage costs have increased exponentially over the last 10 years because most users do not delete their emails. Which of the following can BEST alleviate this issue while not sacrificing security?

- A. Implementing record retention tools and techniques
- B. Establishing e-discovery and data loss prevention (DLP)
- C. Sending notifications when near storage quota
- D. Implementing a bring your own device (BYOD) policy

**Answer:** A

**NEW QUESTION 226**

- (Exam Topic 1)

Improvements in the design and implementation of a control will MOST likely result in an update to:

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

**Answer:** B

**NEW QUESTION 231**

- (Exam Topic 1)

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

- A. Data owner
- B. Control owner

- C. Risk owner
- D. System owner

**Answer:** B

**NEW QUESTION 232**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 236**

- (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 238**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 243**

- (Exam Topic 2)

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 245**

- (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 250**

- (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 254**

- (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 258**

- (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 260**

- (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 263**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 265**

- (Exam Topic 2)

An organization's financial analysis department uses an in-house forecasting application for business projections. Who is responsible for defining access roles to protect the sensitive data within this application?

- A. IT risk manager
- B. IT system owner
- C. Information security manager
- D. Business owner

**Answer:** D

**NEW QUESTION 270**

- (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 272**

- (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 275**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 276**

- (Exam Topic 2)

Which of the following is a KEY outcome of risk ownership?

- A. Risk responsibilities are addressed.
- B. Risk-related information is communicated.
- C. Risk-oriented tasks are defined.
- D. Business process risk is analyzed.

**Answer: A**

**NEW QUESTION 278**

- (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 283**

- (Exam Topic 2)

A bank wants to send a critical payment order via email to one of its offshore branches. Which of the following is the BEST way to ensure the message reaches the intended recipient without alteration?

- A. Add a digital certificate
- B. Apply multi-factor authentication
- C. Add a hash to the message
- D. Add a secret key

**Answer: C**

**NEW QUESTION 287**

- (Exam Topic 2)

Which of the following is MOST important for an organization to have in place when developing a risk management framework?

- A. A strategic approach to risk including an established risk appetite
- B. A risk-based internal audit plan for the organization
- C. A control function within the risk management team
- D. An organization-wide risk awareness training program

**Answer: A**

**NEW QUESTION 290**

- (Exam Topic 2)

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

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

**Answer: D**

**NEW QUESTION 292**

- (Exam Topic 2)

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

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

**Answer:**

D

**NEW QUESTION 295**

- (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 299**

- (Exam Topic 2)

The GREATEST concern when maintaining a risk register is that:

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

**Answer: D**

**NEW QUESTION 304**

- (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 305**

- (Exam Topic 2)

Which of the following BEST helps to identify significant events that could impact an organization? Vulnerability analysis

- A. Control analysis
- B. Scenario analysis
- C. Heat map analysis

**Answer: C**

**NEW QUESTION 309**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 311**

- (Exam Topic 2)

Who should be responsible for implementing and maintaining security controls?

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

**Answer: D**

**NEW QUESTION 316**

- (Exam Topic 2)

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 319**

- (Exam Topic 2)

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:** C

**NEW QUESTION 321**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 323**

- (Exam Topic 2)

The PRIMARY objective of The board of directors periodically reviewing the risk profile is to help ensure:

- A. the risk strategy is appropriate
- B. KRIs and KPIs are aligned
- C. performance of controls is adequate
- D. the risk monitoring process has been established

**Answer:** B

**NEW QUESTION 324**

- (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 326**

- (Exam Topic 2)

Which of the following should be considered when selecting a risk response?

- A. Risk scenarios analysis
- B. Risk response costs
- C. Risk factor awareness
- D. Risk factor identification

**Answer:** B

**NEW QUESTION 330**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 335**

- (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 338**

- (Exam Topic 2)

Management has required information security awareness training to reduce the risk associated with credential compromise. What is the BEST way to assess the effectiveness of the training?

- A. Conduct social engineering testing.
- B. Audit security awareness training materials.
- C. Administer an end-of-training quiz.
- D. Perform a vulnerability assessment.

**Answer:** A

**NEW QUESTION 341**

- (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 343**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 346**

- (Exam Topic 2)

Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

- A. An internal audit
- B. Security operations center review
- C. Internal penetration testing
- D. A third-party audit

**Answer:** A

**NEW QUESTION 350**

- (Exam Topic 2)

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 355**

- (Exam Topic 2)

After identifying new risk events during a project, the project manager's NEXT step should be to:

- A. determine if the scenarios need to be accepted or responded to.
- B. record the scenarios into the risk register.
- C. continue with a qualitative risk analysis.
- D. continue with a quantitative risk analysis.

**Answer:** A

**NEW QUESTION 359**

- (Exam Topic 2)

Which of the following is a KEY responsibility of the second line of defense?

- A. Implementing control activities
- B. Monitoring control effectiveness
- C. Conducting control self-assessments
- D. Owning risk scenarios

**Answer:** B

**NEW QUESTION 364**

- (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 368**

- (Exam Topic 2)

Which of the following would BEST enable mitigation of newly identified risk factors related to internet of Things (IoT)?

- A. Introducing control procedures early in the life cycle
- B. Implementing IoT device software monitoring
- C. Performing periodic risk assessments of IoT
- D. Performing secure code reviews

**Answer:** A

**NEW QUESTION 370**

- (Exam Topic 2)

Which of the following would be MOST helpful to a risk owner when making risk-aware decisions?

- A. Risk exposure expressed in business terms
- B. Recommendations for risk response options
- C. Resource requirements for risk responses
- D. List of business areas affected by the risk

**Answer:** A

**NEW QUESTION 374**

- (Exam Topic 2)

Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

- A. Percentage of business users completing risk training
- B. Percentage of high-risk scenarios for which risk action plans have been developed
- C. Number of key risk indicators (KRIs) defined
- D. Time between when IT risk scenarios are identified and the enterprise's response

**Answer:** C

**NEW QUESTION 378**

- (Exam Topic 2)

Which of the following is the BEST way for a risk practitioner to verify that management has addressed control issues identified during a previous external audit?

- A. Interview control owners.
- B. Observe the control enhancements in operation.
- C. Inspect external audit documentation.
- D. Review management's detailed action plans.

**Answer:** B

**NEW QUESTION 383**

- (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 386**

- (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 390**

- (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 391**

- (Exam Topic 2)

What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium	Low	Low
Tango	Medium	Low	Medium
Uniform	High	High	High
Victor	High	Medium	Medium

- A. Relative positions on the risk map
- B. Risk treatment options
- C. Capability of enterprise to implement
- D. The multiple risk factors addressed by a chosen response

**Answer: A**

**NEW QUESTION 395**

- (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 398**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 400**

- (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 403**

- (Exam Topic 2)

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:** A

**NEW QUESTION 404**

- (Exam Topic 2)

A risk practitioner learns that the organization's industry is experiencing a trend of rising security incidents. Which of the following is the BEST course of action?

- A. Evaluate the relevance of the evolving threats.
- B. Review past internal audit results.
- C. Respond to organizational security threats.
- D. Research industry published studies.

**Answer:** A

**NEW QUESTION 406**

- (Exam Topic 2)

A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

- A. Ask the business to make a budget request to remediate the problem.
- B. Build a business case to remediate the fix.
- C. Research the types of attacks the threat can present.
- D. Determine the impact of the missing threat.

**Answer:** D

**NEW QUESTION 410**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 413**

- (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 415**

- (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 419**

- (Exam Topic 2)

A software developer has administrative access to a production application. Which of the following should be of GREATEST concern to a risk practitioner?

- A. The administrative access does not allow for activity log monitoring.
- B. The administrative access does not follow password management protocols.
- C. The administrative access represents a deviation from corporate policy.



D. The administrative access represents a segregation of duties conflict.

**Answer:** D

**NEW QUESTION 420**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 423**

- (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:** D

**NEW QUESTION 427**

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?

- A. Self-assessments by process owners
- B. Mitigation plan progress reports
- C. Risk owner attestation
- D. Change in the level of residual risk

**Answer:** D

**NEW QUESTION 431**

- (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 433**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 434**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 439**

- (Exam Topic 2)

An IT organization is replacing the customer relationship management (CRM) system. Who should own the risk associated with customer data leakage caused by

insufficient IT security controls for the new system?

- A. Chief information security officer
- B. Business process owner
- C. Chief risk officer
- D. IT controls manager

**Answer:** B

**NEW QUESTION 442**

- (Exam Topic 2)

Which of the following is MOST important to ensure when continuously monitoring the performance of a client-facing application?

- A. Objectives are confirmed with the business owner
- B. Control owners approve control changes.
- C. End-user acceptance testing has been conducted
- D. Performance information in the log is encrypted

**Answer:** D

**NEW QUESTION 443**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 445**

- (Exam Topic 2)

The PRIMARY purpose of IT control status reporting is to:

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

**Answer:** D

**NEW QUESTION 450**

- (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 452**

.....

## 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](#)**