

Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control



NEW QUESTION 1

- (Exam Topic 1)

Which of the following is the FIRST step in managing the risk associated with the leakage of confidential data?

- A. Maintain and review the classified data inventor.
- B. Implement mandatory encryption on data
- C. Conduct an awareness program for data owners and users.
- D. Define and implement a data classification policy

Answer: D

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 3

- (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 4

- (Exam Topic 1)

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

- A. Ongoing availability of data
- B. Ability to aggregate data
- C. Ability to predict trends
- D. Availability of automated reporting systems

Answer: C

NEW QUESTION 5

- (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 6

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 7

- (Exam Topic 1)

A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

- A. Document the finding in the risk register.
- B. Invoke the incident response plan.

- C. Re-evaluate key risk indicators.
- D. Modify the design of the control.

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

Which of the following is the BEST method to identify unnecessary controls?

- A. Evaluating the impact of removing existing controls
- B. Evaluating existing controls against audit requirements
- C. Reviewing system functionalities associated with business processes
- D. Monitoring existing key risk indicators (KRIs)

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Which of the following is the MOST common concern associated with outsourcing to a service provider?

- A. Lack of technical expertise
- B. Combining incompatible duties
- C. Unauthorized data usage
- D. Denial of service attacks

Answer: B

NEW QUESTION 10

- (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 12

- (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 13

- (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 15

- (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 17

- (Exam Topic 1)

Which of the following should be the HIGHEST priority when developing a risk response?

- A. The risk response addresses the risk with a holistic view.
- B. The risk response is based on a cost-benefit analysis.
- C. The risk response is accounted for in the budget.
- D. The risk response aligns with the organization's risk appetite.

Answer: D

NEW QUESTION 22

- (Exam Topic 1)

Which of the following is the MOST important outcome of reviewing the risk management process?

- A. Assuring the risk profile supports the IT objectives
- B. Improving the competencies of employees who performed the review
- C. Determining what changes should be made to IS policies to reduce risk
- D. Determining that procedures used in risk assessment are appropriate

Answer: A

NEW QUESTION 25

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 28

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 31

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 34

- (Exam Topic 1)

Which of the following is the BEST approach to use when creating a comprehensive set of IT risk scenarios?

- A. Derive scenarios from IT risk policies and standards.
- B. Map scenarios to a recognized risk management framework.
- C. Gather scenarios from senior management.
- D. Benchmark scenarios against industry peers.

Answer: A

NEW QUESTION 38

- (Exam Topic 1)

A risk practitioner discovers several key documents detailing the design of a product currently in development have been posted on the Internet. What should be the risk practitioner's FIRST course of action?

- A. invoke the established incident response plan.
- B. Inform internal audit.
- C. Perform a root cause analysis
- D. Conduct an immediate risk assessment

Answer: A

NEW QUESTION 41

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 45

- (Exam Topic 1)

Which of the following will BEST quantify the risk associated with malicious users in an organization?

- A. Business impact analysis
- B. Risk analysis
- C. Threat risk assessment
- D. Vulnerability assessment

Answer: A

NEW QUESTION 50

- (Exam Topic 1)

Reviewing results from which of the following is the BEST way to identify information systems control deficiencies?

- A. Vulnerability and threat analysis
- B. Control remediation planning
- C. User acceptance testing (UAT)
- D. Control self-assessment (CSA)

Answer: D

NEW QUESTION 51

- (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 55

- (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)

The MOST effective way to increase the likelihood that risk responses will be implemented is to:

- A. create an action plan
- B. assign ownership
- C. review progress reports
- D. perform regular audits.

Answer: B

NEW QUESTION 61

- (Exam Topic 1)

A key risk indicator (KRI) is reported to senior management on a periodic basis as exceeding thresholds, but each time senior management has decided to take no action to reduce the risk. Which of the following is the MOST likely reason for senior management's response?

- A. The underlying data source for the KRI is using inaccurate data and needs to be corrected.
- B. The KRI is not providing useful information and should be removed from the KRI inventory.
- C. The KRI threshold needs to be revised to better align with the organization's risk appetite
- D. Senior management does not understand the KRI and should undergo risk training.

Answer: C

NEW QUESTION 62

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 63

- (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 66

- (Exam Topic 1)

Which of the following is the MOST important characteristic of an effective risk management program?

- A. Risk response plans are documented
- B. Controls are mapped to key risk scenarios.
- C. Key risk indicators are defined.
- D. Risk ownership is assigned

Answer: D

NEW QUESTION 67

- (Exam Topic 1)

Which of the following would be the BEST recommendation if the level of risk in the IT risk profile has decreased and is now below management's risk appetite?

- A. Optimize the control environment.
- B. Realign risk appetite to the current risk level.
- C. Decrease the number of related risk scenarios.
- D. Reduce the risk management budget.

Answer: A

NEW QUESTION 69

- (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 74

- (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 76

- (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 80

- (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 83

- (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 86

- (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 88

- (Exam Topic 1)

The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

- A. resources to monitor backups backup
- B. recovery requests
- C. restoration monitoring reports.
- D. recurring restore failures.

Answer: D

NEW QUESTION 91

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 93

- (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 95

- (Exam Topic 1)

Which of the following BEST describes the role of the IT risk profile in strategic IT-related decisions?

- A. It compares performance levels of IT assets to value delivered.
- B. It facilitates the alignment of strategic IT objectives to business objectives.
- C. It provides input to business managers when preparing a business case for new IT projects.
- D. It helps assess the effects of IT decisions on risk exposure

Answer: D

NEW QUESTION 97

- (Exam Topic 1)

Which of the following helps ensure compliance with a nonrepudiation policy requirement for electronic transactions?

- A. Digital signatures
- B. Encrypted passwords
- C. One-time passwords
- D. Digital certificates

Answer: A

NEW QUESTION 100

- (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 103

- (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 107

- (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 110

- (Exam Topic 1)

Risk management strategies are PRIMARILY adopted to:

- A. take necessary precautions for claims and losses.
- B. achieve acceptable residual risk levels.
- C. avoid risk for business and IT assets.
- D. achieve compliance with legal requirements.

Answer: B

NEW QUESTION 111

- (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 112

- (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 115

- (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 118

- (Exam Topic 1)

Which of the following is the BEST method for assessing control effectiveness?

- A. Ad hoc control reporting
- B. Control self-assessment
- C. Continuous monitoring
- D. Predictive analytics

Answer: C

NEW QUESTION 120

- (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 124

- (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 125

- (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 126

- (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 130

- (Exam Topic 2)

The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

- A. assess gaps in IT risk management operations and strategic focus.
- B. confirm that IT risk assessment results are expressed as business impact.
- C. verify implemented controls to reduce the likelihood of threat materialization.
- D. ensure IT risk management is focused on mitigating potential risk.

Answer: A

NEW QUESTION 135

- (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 140

- (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 145

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 150

- (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 155

- (Exam Topic 2)

Which of the following statements BEST describes risk appetite?

- A. The amount of risk an organization is willing to accept
- B. The effective management of risk and internal control environments
- C. Acceptable variation between risk thresholds and business objectives
- D. The acceptable variation relative to the achievement of objectives

Answer:

A

NEW QUESTION 160

- (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 162

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 167

- (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 168

- (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 171

- (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 172

- (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 175

- (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 178

- (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 181

- (Exam Topic 2)

Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

- A. Organizational reporting process
- B. Incident reporting procedures
- C. Regularly scheduled audits
- D. Incident management policy

Answer: C

NEW QUESTION 184

- (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 185

- (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 188

- (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 193

- (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 195

- (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 199

- (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 202

- (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 205

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 210

- (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 213

- (Exam Topic 2)

Which of The following is the PRIMARY consideration when establishing an organization's risk management methodology?

- A. Business context
- B. Risk tolerance level
- C. Resource requirements
- D. Benchmarking information

Answer: A

NEW QUESTION 216

- (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 218

- (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 221

- (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 223

- (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 225

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 226

- (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 229

- (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 233

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 235

- (Exam Topic 2)

An external security audit has reported multiple findings related to control noncompliance. Which of the following would be MOST important for the risk practitioner to communicate to senior management?

- A. A recommendation for internal audit validation
- B. Plans for mitigating the associated risk
- C. Suggestions for improving risk awareness training
- D. The impact to the organization's risk profile

Answer: B

NEW QUESTION 238

- (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 241

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 242

- (Exam Topic 2)

The BEST key performance indicator (KPI) to measure the effectiveness of a vendor risk management program is the percentage of:

- A. vendors providing risk assessments on time.
- B. vendor contracts reviewed in the past year.
- C. vendor risk mitigation action items completed on time.
- D. vendors that have reported control-related incidents.

Answer: C

NEW QUESTION 246

- (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 247

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 251

.....

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](#)