

## Exam Questions CRISC

Certified in Risk and Information Systems Control

<https://www.2passeasy.com/dumps/CRISC/>



#### 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 in the risk register.
- C. Inform senior management.
- D. update the risk response plan.

**Answer: A**

#### NEW QUESTION 3

- (Exam Topic 1)

Which of the following BEST provides an early warning that network access of terminated employees is not being revoked in accordance with the service level agreement (SLA)?

- A. Updating multi-factor authentication
- B. Monitoring key access control performance indicators
- C. Analyzing access control logs for suspicious activity
- D. Revising the service level agreement (SLA)

**Answer: B**

#### NEW QUESTION 4

- (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 5

- (Exam Topic 1)

An organization is planning to engage a cloud-based service provider for some of its data-intensive business processes. Which of the following is MOST important to help define the IT risk associated with this outsourcing activity?

- A. Service level agreement
- B. Customer service reviews
- C. Scope of services provided
- D. Right to audit the provider

**Answer: D**

#### NEW QUESTION 6

- (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 7

- (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 8

- (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 9

- (Exam Topic 1)

Which of the following is the MOST effective key performance indicator (KPI) for change management?

- A. Percentage of changes with a fallback plan
- B. Number of changes implemented
- C. Percentage of successful changes
- D. Average time required to implement a change

**Answer:** C

#### NEW QUESTION 10

- (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)

Periodically reviewing and updating a risk register with details on identified risk factors PRIMARILY helps to:

- A. minimize the number of risk scenarios for risk assessment.
- B. aggregate risk scenarios identified across different business units.
- C. build a threat profile of the organization for management review.
- D. provide a current reference to stakeholders for risk-based decisions.

**Answer:** C

#### NEW QUESTION 11

- (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)

During an IT risk scenario review session, business executives question why they have been assigned ownership of IT-related risk scenarios. They feel IT risk is technical in nature and therefore should be owned by IT. Which of the following is the BEST way for the risk practitioner to address these concerns?

- A. Describe IT risk scenarios in terms of business risk.
- B. Recommend the formation of an executive risk council to oversee IT risk.
- C. Provide an estimate of IT system downtime if IT risk materializes.
- D. Educate business executives on IT risk concepts.

**Answer:** A

#### NEW QUESTION 15

- (Exam Topic 1)

Which of the following is the MOST important data source for monitoring key risk indicators (KRIs)?

- A. Directives from legal and regulatory authorities
- B. Audit reports from internal information systems audits
- C. Automated logs collected from different systems
- D. Trend analysis of external risk factors

**Answer: C**

#### NEW QUESTION 20

- (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 22

- (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 24

- (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 29

- (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 33

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 36

- (Exam Topic 1)

A risk practitioner is organizing a training session to communicate risk assessment methodologies to ensure a consistent risk view within the organization. Which of the following is the MOST important topic to cover in this training?

- A. Applying risk appetite
- B. Applying risk factors
- C. Referencing risk event data
- D. Understanding risk culture

**Answer: D**

**NEW QUESTION 41**

- (Exam Topic 1)

A web-based service provider with a low risk appetite for system outages is reviewing its current risk profile for online security. Which of the following observations would be MOST relevant to escalate to senior management?

- A. An increase in attempted distributed denial of service (DDoS) attacks
- B. An increase in attempted website phishing attacks
- C. A decrease in achievement of service level agreements (SLAs)
- D. A decrease in remediated web security vulnerabilities

**Answer:** A

**NEW QUESTION 45**

- (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 47**

- (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 49**

- (Exam Topic 1)

A risk assessment has identified that an organization may not be in compliance with industry regulations. The BEST course of action would be to:

- A. conduct a gap analysis against compliance criteria.
- B. identify necessary controls to ensure compliance.
- C. modify internal assurance activities to include control validation.
- D. collaborate with management to meet compliance requirements.

**Answer:** A

**NEW QUESTION 50**

- (Exam Topic 1)

Risk mitigation procedures should include:

- A. buying an insurance policy.
- B. acceptance of exposures
- C. deployment of counter measures.
- D. enterprise architecture implementation.

**Answer:** C

**NEW QUESTION 51**

- (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 53**

- (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 58**

- (Exam Topic 1)

An organization has outsourced its IT security operations to a third party. Who is ULTIMATELY accountable for the risk associated with the outsourced operations?

- A. The third party's management
- B. The organization's management
- C. The control operators at the third party
- D. The organization's vendor management office

**Answer: B**

**NEW QUESTION 63**

- (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 65**

- (Exam Topic 1)

Which of the following is the BEST indication of an effective risk management program?

- A. Risk action plans are approved by senior management.
- B. Residual risk is within the organizational risk appetite
- C. Mitigating controls are designed and implemented.
- D. Risk is recorded and tracked in the risk register

**Answer: B**

**NEW QUESTION 68**

- (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 70**

- (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 74**

- (Exam Topic 1)

Which of the following would be MOST helpful when estimating the likelihood of negative events?

- A. Business impact analysis
- B. Threat analysis
- C. Risk response analysis
- D. Cost-benefit analysis

**Answer: B**

**NEW QUESTION 76**

- (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 81**

- (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 83**

- (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 84**

- (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 88**

- (Exam Topic 1)

Which of the following should be the PRIMARY consideration when assessing the automation of control monitoring?

- A. impact due to failure of control
- B. Frequency of failure of control
- C. Contingency plan for residual risk
- D. Cost-benefit analysis of automation

**Answer:** D

**NEW QUESTION 93**

- (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 97**

- (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 102**

- (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 105**

- (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 109**

- (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 111**

- (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 115**

- (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 120**

- (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 125**

- (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 129**

- (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 132

- (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 133

- (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 136

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 140

- (Exam Topic 1)

Which of the following tools is MOST effective in identifying trends in the IT risk profile?

- A. Risk self-assessment
- B. Risk register
- C. Risk dashboard
- D. Risk map

**Answer: C**

#### NEW QUESTION 142

- (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 146

- (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 149**

- (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 153**

- (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 154**

- (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 158**

- (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 160**

- (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 162**

- (Exam Topic 1)

Which of the following will BEST mitigate the risk associated with IT and business misalignment?

- A. Establishing business key performance indicators (KPIs)
- B. Introducing an established framework for IT architecture
- C. Establishing key risk indicators (KRIs)
- D. Involving the business process owner in IT strategy

**Answer: D**

**NEW QUESTION 164**

- (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 168**

- (Exam Topic 1)

Which of the following would be considered a vulnerability?

- A. Delayed removal of employee access
- B. Authorized administrative access to HR files
- C. Corruption of files due to malware
- D. Server downtime due to a denial of service (DoS) attack

**Answer: A**

**NEW QUESTION 171**

- (Exam Topic 1)

An organization has determined a risk scenario is outside the defined risk tolerance level. What should be the NEXT course of action?

- A. Develop a compensating control.
- B. Allocate remediation resources.
- C. Perform a cost-benefit analysis.
- D. Identify risk responses

**Answer: D**

**NEW QUESTION 175**

- (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 177**

- (Exam Topic 1)

A risk assessment has identified that departments have installed their own WiFi access points on the enterprise network. Which of the following would be MOST important to include in a report to senior management?

- A. The network security policy
- B. Potential business impact
- C. The WiFi access point configuration
- D. Planned remediation actions

**Answer: B**

**NEW QUESTION 182**

- (Exam Topic 1)

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

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

**Answer: D**

**NEW QUESTION 184**

- (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 186**

- (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 190**

- (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 195**

- (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 200**

- (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 201**

- (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 206**

- (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 208**

- (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 213**

- (Exam Topic 1)

During the risk assessment of an organization that processes credit cards, a number of existing controls have been found to be ineffective and do not meet

industry standards. The overall control environment may still be effective if:

- A. compensating controls are in place.
- B. a control mitigation plan is in place.
- C. risk management is effective.
- D. residual risk is accepted.

**Answer:** A

#### NEW QUESTION 217

- (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 222

- (Exam Topic 1)

A rule-based data loss prevention (DLP) tool has recently been implemented to reduce the risk of sensitive data leakage. Which of the following is MOST likely to change as a result of this implementation?

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

**Answer:** A

#### NEW QUESTION 223

- (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 226

- (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 229

- (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 233

- (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 235**

- (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 239**

- (Exam Topic 2)

Which of the following is MOST important when discussing risk within an organization?

- A. Adopting a common risk taxonomy
- B. Using key performance indicators (KPIs)
- C. Creating a risk communication policy
- D. Using key risk indicators (KRIs)

**Answer: A**

**NEW QUESTION 244**

- (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 247**

- (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 252**

- (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 256**

- (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 258**

- (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 262**

- (Exam Topic 2)

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

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

Answer: C

**NEW QUESTION 265**

- (Exam Topic 2)

Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

- A. Align business objectives with risk appetite.
- B. Enable risk-based decision making.
- C. Design and implement risk response action plans.
- D. Update risk responses in the risk register

Answer: B

**NEW QUESTION 270**

- (Exam Topic 2)

Whose risk tolerance matters MOST when making a risk decision?

- A. Customers who would be affected by a breach
- B. Auditors, regulators and standards organizations
- C. The business process owner of the exposed assets
- D. The information security manager

Answer: C

**NEW QUESTION 271**

- (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 276**

- (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 280**

- (Exam Topic 2)

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

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

Answer: A

**NEW QUESTION 285**

- (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 286**

- (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 289**

- (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 292**

- (Exam Topic 2)

Which of the following is MOST important to review when determining whether a potential IT service provider s control environment is effective?

- A. Independent audit report
- B. Control self-assessment
- C. Key performance indicators (KPIs)
- D. Service level agreements (SLAs)

**Answer:** A

**NEW QUESTION 295**

- (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 297**

- (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 299**

- (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 301**

- (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 305

- (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 306

- (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 311

- (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 312

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 315

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 316

- (Exam Topic 2)

A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?

- A. Reviewing access control lists
- B. Authorizing user access requests
- C. Performing user access recertification
- D. Terminating inactive user access

**Answer: B**

**NEW QUESTION 318**

- (Exam Topic 2)

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

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

**Answer: D**

**NEW QUESTION 321**

- (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 analysis 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 322**

- (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 327**

- (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 331**

- (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 336**

- (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 337**

- (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 341**

- (Exam Topic 2)

Which of the following is the FIRST step in risk assessment?

- A. Review risk governance
- B. Asset identification
- C. Identify risk factors
- D. Inherent risk identification

**Answer: B**

**NEW QUESTION 345**

- (Exam Topic 2)

Which of the following is MOST important to the integrity of a security log?

- A. Least privilege access
- B. Inability to edit
- C. Ability to overwrite
- D. Encryption

**Answer: A**

**NEW QUESTION 348**

- (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 352**

- (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 355**

- (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 359**

- (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 364**

- (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 367**

- (Exam Topic 2)

Which of the following is MOST helpful in verifying that the implementation of a risk mitigation control has been completed as intended?

- A. An updated risk register
- B. Risk assessment results
- C. Technical control validation
- D. Control testing results

**Answer: D**

**NEW QUESTION 370**

- (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 372**

- (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 373**

- (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 375**

- (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 379**

- (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 382**

- (Exam Topic 2)

Which of the following is MOST important to understand when developing key risk indicators (KRIs)?

- A. KRI thresholds

- B. Integrity of the source data
- C. Control environment
- D. Stakeholder requirements

**Answer:** A

**NEW QUESTION 385**

- (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 388**

- (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 392**

- (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 396**

- (Exam Topic 2)

What should be the PRIMARY objective for a risk practitioner performing a post-implementation review of an IT risk mitigation project?

- A. Documenting project lessons learned
- B. Validating the risk mitigation project has been completed
- C. Confirming that the project budget was not exceeded
- D. Verifying that the risk level has been lowered

**Answer:** A

**NEW QUESTION 397**

- (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 401**

- (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 404**

- (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 409

- (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 412

- (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 415

- (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 417

- (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 418

- (Exam Topic 2)

An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

- A. IT infrastructure head
- B. Human resources head
- C. Supplier management head
- D. Application development head

**Answer:** B

#### NEW QUESTION 421

- (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 422**

- (Exam Topic 2)

To help ensure all applicable risk scenarios are incorporated into the risk register, it is MOST important to review the:

- A. risk mitigation approach
- B. cost-benefit analysis.
- C. risk assessment results.
- D. vulnerability assessment results

**Answer: C**

**NEW QUESTION 425**

- (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 430**

- (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 433**

- (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 435**

- (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 438**

- (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 440**

- (Exam Topic 2)

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

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

Answer: D

**NEW QUESTION 443**

- (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 444**

- (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 446**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CRISC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CRISC Product From:

<https://www.2passeasy.com/dumps/CRISC/>

### Money Back Guarantee

#### **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