

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 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)

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 3

- (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 4

- (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 5

- (Exam Topic 1)

Which of the following would BEST help an enterprise prioritize risk scenarios?

- A. Industry best practices
- B. Placement on the risk map
- C. Degree of variances in the risk
- D. Cost of risk mitigation

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

A risk practitioner is summarizing the results of a high-profile risk assessment sponsored by senior management. The BEST way to support risk-based decisions by senior management would be to:

- A. map findings to objectives.
- B. provide a quantified detailed analysts.
- C. recommend risk tolerance thresholds.
- D. quantify key risk indicators (KRIs).

Answer: A

NEW QUESTION 7

- (Exam Topic 1)

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

- A. two-factor authentication.
- B. continuous data backup controls.

- C. encryption for data at rest.
- D. encryption for data in motion.

Answer: B

NEW QUESTION 8

- (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 9

- (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 10

- (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 10

- (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 14

- (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 15

- (Exam Topic 1)

Which of the following would BEST provide early warning of a high-risk condition?

- A. Risk register
- B. Risk assessment
- C. Key risk indicator (KRI)
- D. Key performance indicator (KPI)

Answer: C

NEW QUESTION 17

- (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 22

- (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 23

- (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 25

- (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 30

- (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 34

- (Exam Topic 1)

Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?

- A. Assess the vulnerability management process.
- B. Conduct a control self-assessment.
- C. Conduct a vulnerability assessment.
- D. Reassess the inherent risk of the target.

Answer: C

NEW QUESTION 38

- (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 42

- (Exam Topic 1)

Which of the following is the MOST important consideration for a risk practitioner when making a system implementation go-live recommendation?

- A. Completeness of system documentation
- B. Results of end user acceptance testing
- C. Variances between planned and actual cost
- D. availability of in-house resources

Answer: B

NEW QUESTION 43

- (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 48

- (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 51

- (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 52

- (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 54

- (Exam Topic 1)

Which of the following is MOST effective against external threats to an organizations confidential information?

- A. Single sign-on
- B. Data integrity checking
- C. Strong authentication
- D. Intrusion detection system

Answer: C

NEW QUESTION 57

- (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 60

- (Exam Topic 1)

An organization has allowed its cyber risk insurance to lapse while seeking a new insurance provider. The risk practitioner should report to management that the risk has been:

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

Answer: C

NEW QUESTION 62

- (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 66

- (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 68

- (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 72

- (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 76

- (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 81

- (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 85

- (Exam Topic 1)

Which of the following techniques would be used during a risk assessment to demonstrate to stakeholders that all known alternatives were evaluated?

- A. Control chart
- B. Sensitivity analysis
- C. Trend analysis
- D. Decision tree

Answer: D

NEW QUESTION 89

- (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 90

- (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 92

- (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 95

- (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 99

- (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 104

- (Exam Topic 2)

Which of the following BEST indicates whether security awareness training is effective?

- A. User self-assessment
- B. User behavior after training
- C. Course evaluation
- D. Quality of training materials

Answer: B

NEW QUESTION 107

- (Exam Topic 2)

Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

- A. Compliance breaches are addressed in a timely manner.
- B. Risk ownership is identified and assigned.
- C. Risk treatment options receive adequate funding.
- D. Residual risk is within risk tolerance.

Answer: D

NEW QUESTION 111

- (Exam Topic 2)

A large organization is replacing its enterprise resource planning (ERP) system and has decided not to deploy the payroll module of the new system. Instead, the current payroll system will continue to be used. Of the following, who should own the risk if the ERP and payroll system fail to operate as expected?

- A. The business owner
- B. The ERP administrator
- C. The project steering committee
- D. The IT project manager

Answer: A

NEW QUESTION 112

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 117

- (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 120

- (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 125

- (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 130

- (Exam Topic 2)

Which of the following should be the PRIMARY objective of a risk awareness training program?

- A. To enable risk-based decision making
- B. To promote awareness of the risk governance function
- C. To clarify fundamental risk management principles
- D. To ensure sufficient resources are available

Answer: A

NEW QUESTION 132

- (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 137

- (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 142

- (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 144

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 146

- (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 149

- (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 153

- (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 158

- (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 159

- (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 164

- (Exam Topic 2)

Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?

- A. A companion of risk assessment results to the desired state
- B. A quantitative presentation of risk assessment results
- C. An assessment of organizational maturity levels and readiness
- D. A qualitative presentation of risk assessment results

Answer: D

NEW QUESTION 169

- (Exam Topic 2)

During the initial risk identification process for a business application, it is MOST important to include which of the following stakeholders?

- A. Business process owners
- B. Business process consumers
- C. Application architecture team
- D. Internal audit

Answer: A

NEW QUESTION 174

- (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 178

- (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 179

- (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 182

- (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 187

- (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 188

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 193

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 197

- (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 201

- (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 204

- (Exam Topic 2)

An IT operations team implements disaster recovery controls based on decisions from application owners regarding the level of resiliency needed. Who is the risk owner in this scenario?

- A. Business resilience manager
- B. Disaster recovery team lead
- C. Application owner
- D. IT operations manager

Answer: C

NEW QUESTION 206

- (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 211

- (Exam Topic 2)

A risk practitioner has just learned about new done FIRST?

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

Answer: B

NEW QUESTION 213

- (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 214

- (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 215

- (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 218

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 222

- (Exam Topic 2)

Which of the following is the BEST way to support communication of emerging risk?

- A. Update residual risk levels to reflect the expected risk impact.
- B. Adjust inherent risk levels upward.
- C. Include it on the next enterprise risk committee agenda.
- D. Include it in the risk register for ongoing monitoring.

Answer: D

NEW QUESTION 224

.....

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 FirstTry
- * CRISC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year