

CRISC Dumps

Certified in Risk and Information Systems Control

<https://www.certleader.com/CRISC-dumps.html>



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 4

- (Exam Topic 1)

A risk practitioner is assisting with the preparation of a report on the organization's disaster recovery (DR) capabilities. Which information would have the MOST impact on the overall recovery profile?

- A. The percentage of systems meeting recovery target times has increased.
- B. The number of systems tested in the last year has increased.
- C. The number of systems requiring a recovery plan has increased.
- D. The percentage of systems with long recovery target times has decreased.

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

After a high-profile systems breach at an organization's key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:

After a high-profile systems breach at an organization's key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:

Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

Type	Scope	Completed By
External audit	Financial systems and processes	Third party
Internal audit	IT security risk management	Vendor
Vendor performance scorecard	Service level agreement compliance	Organization
Regulatory examination	Information security management program	Regulator

- A. External audit
- B. Internal audit
- C. Vendor performance scorecard
- D. Regulatory examination

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 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 is the MOST cost-effective way to test a business continuity plan?

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

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 13

- (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 17

- (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 22

- (Exam Topic 1)

Malware has recently affected an organization, The MOST effective way to resolve this situation and define a comprehensive risk treatment plan would be to perform:

- A. a gap analysis
- B. a root cause analysis.
- C. an impact assessment.
- D. a vulnerability assessment.

Answer: C

NEW QUESTION 24

- (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 27

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 28

- (Exam Topic 1)

Which of the following should be the risk practitioner s PRIMARY focus when determining whether controls are adequate to mitigate risk?

- A. Sensitivity analysis
- B. Level of residual risk
- C. Cost-benefit analysis
- D. Risk appetite

Answer: C

NEW QUESTION 30

- (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 33

- (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 35

- (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 40

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 41

- (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 45

- (Exam Topic 1)

Which of the following is the MOST important consideration when multiple risk practitioners capture risk scenarios in a single risk register?

- A. Aligning risk ownership and control ownership
- B. Developing risk escalation and reporting procedures
- C. Maintaining up-to-date risk treatment plans
- D. Using a consistent method for risk assessment

Answer: D

NEW QUESTION 46

- (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 51

- (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 54

- (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 57

- (Exam Topic 1)

The PRIMARY objective for selecting risk response options is to:

- A. reduce risk to an acceptable level.
- B. identify compensating controls.
- C. minimize residual risk.
- D. reduce risk factors.

Answer: A

NEW QUESTION 58

- (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 62

- (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 65

- (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 68

- (Exam Topic 1)

Which of the following controls will BEST detect unauthorized modification of data by a database administrator?

- A. Reviewing database access rights
- B. Reviewing database activity logs
- C. Comparing data to input records
- D. Reviewing changes to edit checks

Answer: B

NEW QUESTION 73

- (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 77

- (Exam Topic 1)

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

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

Answer:

B

NEW QUESTION 81

- (Exam Topic 1)

The PRIMARY reason a risk practitioner would be interested in an internal audit report is to:

- A. plan awareness programs for business managers.
- B. evaluate maturity of the risk management process.
- C. assist in the development of a risk profile.
- D. maintain a risk register based on noncompliances.

Answer: C

NEW QUESTION 86

- (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 90

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 94

- (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 98

- (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 103

- (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 106

- (Exam Topic 1)

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

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

D. Consult with the business owner to update the BCP

Answer: A

NEW QUESTION 107

- (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 112

- (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 113

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 117

- (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 118

- (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 122

- (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 126

- (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 130

- (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 132

- (Exam Topic 1)

An organization has procured a managed hosting service and just discovered the location is likely to be flooded every 20 years. Of the following, who should be notified of this new information FIRST.

- A. The risk owner who also owns the business service enabled by this infrastructure
- B. The data center manager who is also employed under the managed hosting services contract
- C. The site manager who is required to provide annual risk assessments under the contract
- D. The chief information officer (CIO) who is responsible for the hosted services

Answer: A

NEW QUESTION 133

- (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 138

- (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 143

- (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 148

- (Exam Topic 1)

Which of the following would BEST ensure that identified risk scenarios are addressed?

- A. Reviewing the implementation of the risk response
- B. Creating a separate risk register for key business units
- C. Performing real-time monitoring of threats
- D. Performing regular risk control self-assessments

Answer: A

NEW QUESTION 149

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 153

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 156

- (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 158

- (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 159

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 160

- (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 161

- (Exam Topic 1)

Which of the following is MOST critical when designing controls?

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

Answer: B

NEW QUESTION 163

- (Exam Topic 1)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery plan (DRP)?

- A. Number of users that participated in the DRP testing
- B. Number of issues identified during DRP testing
- C. Percentage of applications that met the RTO during DRP testing
- D. Percentage of issues resolved as a result of DRP testing

Answer: B

NEW QUESTION 167

- (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 172

- (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 173

- (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 178

- (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 180

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 181

- (Exam Topic 1)

In addition to the risk register, what should a risk practitioner review to develop an understanding of the organization's risk profile?

- A. The control catalog
- B. The asset profile
- C. Business objectives
- D. Key risk indicators (KRIs)

Answer: C

NEW QUESTION 186

- (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 190

- (Exam Topic 1)

An organization has identified a risk exposure due to weak technical controls in a newly implemented HR system. The risk practitioner is documenting the risk in the risk register. The risk should be owned by the:

- A. chief risk officer.
- B. project manager.
- C. chief information officer.
- D. business process owner.

Answer: D

NEW QUESTION 193

- (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 196

- (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 200

- (Exam Topic 2)

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

- A. Alignment with regulatory requirements
- B. Availability of qualitative data
- C. Properly set thresholds
- D. Alignment with industry benchmarks

Answer: C

NEW QUESTION 205

- (Exam Topic 2)

When reviewing a risk response strategy, senior management's PRIMARY focus should be placed on the:

- A. cost-benefit analysis.
- B. investment portfolio.
- C. key performance indicators (KPIs).
- D. alignment with risk appetite.

Answer: A

NEW QUESTION 208

- (Exam Topic 2)

Controls should be defined during the design phase of system development because:

- A. it is more cost-effective to determine controls in the early design phase.

- B. structured analysis techniques exclude identification of controls.
- C. structured programming techniques require that controls be designed before coding begins.
- D. technical specifications are defined during this phase.

Answer: D

NEW QUESTION 210

- (Exam Topic 2)

Which of the following 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 212

- (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 214

- (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 215

- (Exam Topic 2)

The BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability remediation program is the number of:

- A. vulnerability scans.
- B. recurring vulnerabilities.
- C. vulnerabilities remediated,
- D. new vulnerabilities identified.

Answer: C

NEW QUESTION 217

- (Exam Topic 2)

An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

- A. identify key risk indicators (KRIs) for ongoing monitoring
- B. validate the CTO's decision with the business process owner
- C. update the risk register with the selected risk response
- D. recommend that the CTO revisit the risk acceptance decision.

Answer: A

NEW QUESTION 222

- (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 225

- (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 228

- (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 230

- (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 235

- (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 237

- (Exam Topic 2)

When prioritizing risk response, management should FIRST:

- A. evaluate the organization's ability and expertise to implement the solution.
- B. evaluate the risk response of similar organizations.
- C. address high risk factors that have efficient and effective solutions.
- D. determine which risk factors have high remediation costs

Answer: C

NEW QUESTION 239

- (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 244

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 246

- (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 250

- (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 253

- (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 256

- (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 259

- (Exam Topic 2)

A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

- A. Determine changes in the risk level.
- B. Outsource the vulnerability management process.
- C. Review the patch management process.
- D. Add agenda item to the next risk committee meeting.

Answer: C

NEW QUESTION 262

- (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 266

- (Exam Topic 2)

An upward trend in which of the following metrics should be of MOST concern?

- A. Number of business change management requests
- B. Number of revisions to security policy

- C. Number of security policy exceptions approved
- D. Number of changes to firewall rules

Answer: C

NEW QUESTION 270

- (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 272

- (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 274

- (Exam Topic 2)

A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?

- A. Review the design of the machine learning model against control objectives.
- B. Adopt the machine learning model as a replacement for current manual access reviews.
- C. Ensure the model assists in meeting regulatory requirements for access controls.
- D. Discourage the use of emerging technologies in key processes.

Answer: A

NEW QUESTION 278

- (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 281

- (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 283

- (Exam Topic 2)

Which of the following BEST helps to balance the costs and benefits of managing IT risk?

- A. Prioritizing risk responses
- B. Evaluating risk based on frequency and probability
- C. Considering risk factors that can be quantified
- D. Managing the risk by using controls

Answer: A

NEW QUESTION 286

- (Exam Topic 2)

Which of the following would prompt changes in key risk indicator (KRI) thresholds?

- A. Changes to the risk register
- B. Changes in risk appetite or tolerance
- C. Modification to risk categories
- D. Knowledge of new and emerging threats

Answer: B

NEW QUESTION 291

- (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 296

- (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 297

- (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 301

- (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 305

- (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 307

- (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 309

- (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 310

- (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 312

- (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 316

- (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 319

- (Exam Topic 2)

A risk owner should be the person accountable for:

- A. the risk management process
- B. managing controls.
- C. implementing actions.
- D. the business process.

Answer: D

NEW QUESTION 321

- (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 326

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 328

- (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 329

- (Exam Topic 2)

Which of the following is MOST important for an organization that wants to reduce IT operational risk?

- A. Increasing senior management's understanding of IT operations
- B. Increasing the frequency of data backups
- C. Minimizing complexity of IT infrastructure
- D. Decentralizing IT infrastructure

Answer: D

NEW QUESTION 334

- (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 338

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 340

- (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 342

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk responses have been executed according to their risk action plans?

- A. Risk policy review
- B. Business impact analysis (BIA)
- C. Control catalog
- D. Risk register

Answer: D

NEW QUESTION 346

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 351

- (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 352

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CRISC Exam with Our Prep Materials Via below:

<https://www.certleader.com/CRISC-dumps.html>