



Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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)

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 3

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 4

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 5

- (Exam Topic 1)

Establishing and organizational code of conduct is an example of which type of control?

- A. Preventive
- B. Directive
- C. Detective
- D. Compensating

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 7

- (Exam Topic 1)

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

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

D. high risk tolerance

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

A systems interruption has been traced to a personal USB device plugged into the corporate network by an IT employee who bypassed internal control procedures. Of the following, who should be accountable?

- A. Business continuity manager (BCM)
- B. Human resources manager (HRM)
- C. Chief risk officer (CRO)
- D. Chief information officer (CIO)

Answer: D

NEW QUESTION 9

- (Exam Topic 1)

Which of the following will BEST help mitigate the risk associated with malicious functionality in outsourced application development?

- A. Perform an m-depth code review with an expert
- B. Validate functionality by running in a test environment
- C. Implement a service level agreement.
- D. Utilize the change management process.

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 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 11

- (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 15

- (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 17

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 22

- (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 24

- (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 27

- (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 31

- (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 36

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 38

- (Exam Topic 1)

The PRIMARY advantage of implementing an IT risk management framework is the:

- A. establishment of a reliable basis for risk-aware decision making.
- B. compliance with relevant legal and regulatory requirements.
- C. improvement of controls within the organization and minimized losses.
- D. alignment of business goals with IT objectives.

Answer: A

NEW QUESTION 39

- (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 43

- (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 44

- (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 48

- (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 52

- (Exam Topic 1)

Which of the following is the PRIMARY factor in determining a recovery time objective (RTO)?

- A. Cost of offsite backup premises
- B. Cost of downtime due to a disaster
- C. Cost of testing the business continuity plan
- D. Response time of the emergency action plan

Answer: B

NEW QUESTION 55

- (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 56

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 59

- (Exam Topic 1)

Which of the following is the MOST important consideration when developing an organization's risk taxonomy?

- A. Leading industry frameworks
- B. Business context
- C. Regulatory requirements
- D. IT strategy

Answer: C

NEW QUESTION 61

- (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 66

- (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 67

- (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 72

- (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 77

- (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 82

- (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 83

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 88

- (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 91

- (Exam Topic 1)

Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

- A. Percentage of unpatched IT assets
- B. Percentage of IT assets without ownership
- C. The number of IT assets securely disposed during the past year
- D. The number of IT assets procured during the previous month

Answer: B

NEW QUESTION 94

- (Exam Topic 1)

An organization that has been the subject of multiple social engineering attacks is developing a risk awareness program. The PRIMARY goal of this program should be to:

- A. reduce the risk to an acceptable level.
- B. communicate the consequences for violations.
- C. implement industry best practices.
- D. reduce the organization's risk appetite

Answer: B

NEW QUESTION 97

- (Exam Topic 1)

Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:

- A. a threat.
- B. a vulnerability.
- C. an impact
- D. a control.

Answer: A

NEW QUESTION 101

- (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 102

- (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 104

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 108

- (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 113

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 117

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 120

- (Exam Topic 1)

Which of the following is the MOST useful indicator to measure the efficiency of an identity and access management process?

- A. Number of tickets for provisioning new accounts
- B. Average time to provision user accounts
- C. Password reset volume per month
- D. Average account lockout time

Answer: C

NEW QUESTION 123

- (Exam Topic 1)

When reviewing management's IT control self-assessments, a risk practitioner noted an ineffective control that links to several low residual risk scenarios. What should be the NEXT course of action?

- A. Assess management's risk tolerance.
- B. Recommend management accept the low risk scenarios.
- C. Propose mitigating controls
- D. Re-evaluate the risk scenarios associated with the control

Answer: D

NEW QUESTION 124

- (Exam Topic 1)

Which of the following aspects of an IT risk and control self-assessment would be MOST important to include in a report to senior management?

- A. Changes in control design
- B. A decrease in the number of key controls
- C. Changes in control ownership
- D. An increase in residual risk

Answer: D

NEW QUESTION 126

- (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 129

- (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 134

- (Exam Topic 1)

Which of the following is the FIRST step in managing the security risk associated with wearable technology in the workplace?

- A. Identify the potential risk.
- B. Monitor employee usage.
- C. Assess the potential risk.
- D. Develop risk awareness training.

Answer: A

NEW QUESTION 139

- (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 142

- (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 143

- (Exam Topic 1)

Which of the following is MOST helpful to ensure effective security controls for a cloud service provider?

- A. A control self-assessment
- B. A third-party security assessment report
- C. Internal audit reports from the vendor
- D. Service level agreement monitoring

Answer:

B

NEW QUESTION 144

- (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 146

- (Exam Topic 1)

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

- A. Data owner
- B. Control owner
- C. Risk owner
- D. System owner

Answer: B

NEW QUESTION 147

- (Exam Topic 1)

Who is the MOST appropriate owner for newly identified IT risk?

- A. The manager responsible for IT operations that will support the risk mitigation efforts
- B. The individual with authority to commit organizational resources to mitigate the risk
- C. A project manager capable of prioritizing the risk remediation efforts
- D. The individual with the most IT risk-related subject matter knowledge

Answer: B

NEW QUESTION 152

- (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 156

- (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 160

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 163

- (Exam Topic 2)

The PRIMARY reason for establishing various Threshold levels for a set of key risk indicators (KRIs) is to:

- A. highlight trends of developing risk.
- B. ensure accurate and reliable monitoring.
- C. take appropriate actions in a timely manner.
- D. set different triggers for each stakeholder.

Answer: B

NEW QUESTION 164

- (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 168

- (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 173

- (Exam Topic 2)

Who is PRIMARILY accountable for risk treatment decisions?

- A. Risk owner
- B. Business manager
- C. Data owner
- D. Risk manager

Answer: B

NEW QUESTION 174

- (Exam Topic 2)

Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

- A. To enable consistent data on risk to be obtained
- B. To allow for proper review of risk tolerance
- C. To identify dependencies for reporting risk
- D. To provide consistent and clear terminology

Answer: C

NEW QUESTION 179

- (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 182

- (Exam Topic 2)

An organization's 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 185

- (Exam Topic 2)

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

- A. IT risk manager

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

Answer: D

NEW QUESTION 190

- (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 194

- (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 196

- (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 199

- (Exam Topic 2)

When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:

- A. risk appetite.
- B. security policies
- C. process maps.
- D. risk tolerance level

Answer: B

NEW QUESTION 202

- (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 206

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 211

- (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 214

- (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 216

- (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 219

- (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 224

- (Exam Topic 2)

As part of an overall IT risk management plan, an IT risk register **BEST** helps management:

- A. align IT processes with business objectives.
- B. communicate the enterprise risk management policy.
- C. stay current with existing control status.
- D. understand the organizational risk profile.

Answer: D

NEW QUESTION 229

- (Exam Topic 2)

Which of the following would require updates to an organization's IT risk register?

- A. Discovery of an ineffectively designed key IT control
- B. Management review of key risk indicators (KRIs)
- C. Changes to the team responsible for maintaining the register
- D. Completion of the latest internal audit

Answer: A

NEW QUESTION 233

- (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 235

- (Exam Topic 2)

An organization with a large number of applications wants to establish a security risk assessment program. Which of the following would provide the MOST useful information when determining the frequency of risk assessments?

- A. Feedback from end users
- B. Results of a benchmark analysis
- C. Recommendations from internal audit
- D. Prioritization from business owners

Answer: D

NEW QUESTION 238

- (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 243

- (Exam Topic 2)

Which of the following is a detective control?

- A. Limit check
- B. Periodic access review
- C. Access control software
- D. Rerun procedures

Answer: B

NEW QUESTION 244

- (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 245

- (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 248

- (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 253

- (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 254

- (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 259

- (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 261

- (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 265

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 266

- (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 268

- (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 273

- (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 275

- (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 277

- (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 279

- (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 283

- (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 286

- (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 288

- (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 293

- (Exam Topic 2)

Following a significant change to a business process, a risk practitioner believes the associated risk has been reduced. The risk practitioner should advise the risk owner to FIRST

- A. review the key risk indicators.
- B. conduct a risk analysis.
- C. update the risk register
- D. reallocate risk response resources.

Answer: B

NEW QUESTION 298

- (Exam Topic 2)

The BEST criteria when selecting a risk response is the:

- A. capability to implement the response
- B. importance of IT risk within the enterprise
- C. effectiveness of risk response options
- D. alignment of response to industry standards

Answer: C

NEW QUESTION 299

- (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 304

- (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 308

- (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 311

- (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 314

- (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 319

- (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 323

- (Exam Topic 2)

An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?

- A. Implement IT systems in alignment with business objectives.
- B. Review metrics and key performance indicators (KPIs).
- C. Review design documentation of IT systems.
- D. Evaluate compliance with legal and regulatory requirements.

Answer: B

NEW QUESTION 326

.....

Relate Links

100% Pass Your CRISC Exam with Exam Bible Prep Materials

<https://www.exambible.com/CRISC-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>