Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (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 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)
An organization is planning to engage a cloud-based service provider for some of its data-intensive business processes. Which of the following is MOST important to help define the IT risk associated with this outsourcing activity?

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

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
What is the BEST information to present to business control owners when justifying costs related to controls?

A. Loss event frequency and magnitude
B. The previous year's budget and actuals
C. Industry benchmarks and standards
D. Return on IT security-related investments

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
Which of the following would be a risk practitioners BEST recommendation for preventing cyber intrusion?

A. Establish a cyber response plan
B. Implement data loss prevention (DLP) tools.
C. Implement network segregation.
D. Strengthen vulnerability remediation efforts.

Answer: D

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)
When using a third party to perform penetration testing, which of the following is the MOST important control to minimize operational impact?

A. Perform a background check on the vendor.
B. Require the vendor to sign a nondisclosure agreement.
C. Require the vendor to have liability insurance.

D. Clearly define the project scope

Answer: D

NEW QUESTION 8
- (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 9
- (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)
A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

A. Document the finding in the risk register.
B. Invoke the incident response plan.
C. Re-evaluate key risk indicators.
D. Modify the design of the control.

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

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

Answer: A

NEW QUESTION 14
- (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 17
- (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 19
- (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 21
- (Exam Topic 1)
Which of the following is the MOST common concern associated with outsourcing to a service provider?

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

Answer: B

NEW QUESTION 26
- (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 29
- (Exam Topic 1)
Which of the following is the MOST important data source for monitoring key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 31
- (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 36
- (Exam Topic 1)
The PRIMARY benefit of maintaining an up-to-date risk register is that it helps to:

A. implement uniform controls for common risk scenarios.
B. ensure business unit risk is uniformly distributed.
C. build a risk profile for management review.
D. quantify the organization's risk appetite.

Answer: C

NEW QUESTION 41
- (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 45
- (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 nude to IS policies to reduce risk
D. Determining that procedures used in risk assessment are appropriate

Answer: A

NEW QUESTION 50
- (Exam Topic 1)
A web-based service provider with a low risk appetite for system outages is reviewing its current risk profile for online security. Which of the following observations would be MOST relevant to escalate to senior management?

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

Answer: A

NEW QUESTION 54
- (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 BES 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 59
- (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 61
- (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 64
- (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 68
- (Exam Topic 1)
An organization has outsourced its IT security operations to a third party. Who is ULTIMATELY accountable for the risk associated with the outsourced operations?

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

Answer: B

NEW QUESTION 70
- (Exam Topic 1)
Which of the following is the BEST approach to use when creating a comprehensive set of IT risk scenarios?

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

Answer: A

NEW QUESTION 71
- (Exam Topic 1)
The PRIMARY objective for selecting risk response options is to:

A. reduce risk 10 an acceptable level.
B. identify compensating controls.
C. minimize residual risk.
D. reduce risk factors.

Answer: A

NEW QUESTION 75
- (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 77
- (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 78
- (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 81
- (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 85
- (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 90
- (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 93
- (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 98
- (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 101
- (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 104
- (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 109
- (Exam Topic 1)
In an organization with a mature risk management program, which of the following would provide the BEST evidence that the IT risk profile is up to date?

A. Risk questionnaire
B. Risk register
C. Management assertion
D. Compliance manual

Answer: B

NEW QUESTION 113
- (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 114
- (Exam Topic 1)
When updating the risk register after a risk assessment, which of the following is MOST important to include?

A. Historical losses due to past risk events
B. Cost to reduce the impact and likelihood
C. Likelihood and impact of the risk scenario
D. Actor and threat type of the risk scenario

Answer: C

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 119
- (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)
Who should be accountable for ensuring effective cybersecurity controls are established?

A. Risk owner
B. Security management function
C. IT management
D. Enterprise risk function

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 131
- (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 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 134
- (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 135
- (Exam Topic 1)
Which of the following would BEST help to ensure that identified risk is efficiently managed?

A. Reviewing the maturity of the control environment
B. Regularly monitoring the project plan
C. Maintaining a key risk indicator for each asset in the risk register
D. Periodically reviewing controls per the risk treatment plan

Answer: D

NEW QUESTION 136
- (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 141
- (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 146
- (Exam Topic 1)
The BEST way to justify the risk mitigation actions recommended in a risk assessment would be to:

A. align with audit results.
B. benchmark with competitor s actions.
C. reference best practice.
D. focus on the business drivers

Answer: D

NEW QUESTION 147
- (Exam Topic 1)
Which of the following should be included in a risk scenario to be used for risk analysis?

A. Risk appetite
B. Threat type
C. Risk tolerance
D. Residual risk

Answer: B

NEW QUESTION 149

- (Exam Topic 1)
Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

A. Updating the risk register to include the risk mitigation plan
B. Determining processes for monitoring the effectiveness of the controls
C. Ensuring that control design reduces risk to an acceptable level
D. Confirming to management the controls reduce the likelihood of the risk

Answer: A

NEW QUESTION 152
- (Exam Topic 1)
Which of the following would be the BEST way to help ensure the effectiveness of a data loss prevention (DLP) control that has been implemented to prevent the loss of credit card data?

A. Testing the transmission of credit card numbers
B. Reviewing logs for unauthorized data transfers
C. Configuring the DLP control to block credit card numbers
D. Testing the DLP rule change control process

Answer: A

NEW QUESTION 157
- (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 158
- (Exam Topic 1)
The BEST reason to classify IT assets during a risk assessment is to determine the:

A. priority in the risk register.
B. business process owner.
C. enterprise risk profile.
D. appropriate level of protection.

Answer: D

NEW QUESTION 163
- (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 167
- (Exam Topic 1)
Which of the following issues should be of GREATEST concern when evaluating existing controls during a risk assessment?

A. A high number of approved exceptions exist with compensating controls.
B. Successive assessments have the same recurring vulnerabilities.
C. Redundant compensating controls are in place.
D. Asset custodians are responsible for defining controls instead of asset owners.

Answer: D

NEW QUESTION 172
- (Exam Topic 1)
A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application. Who should have the authority to accept the associated risk?

A. Business continuity director
B. Disaster recovery manager
C. Business application owner
D. Data center manager

Answer: C

NEW QUESTION 173
- (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 175
- (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 176
- (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 178
- (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 181
- (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 185
- (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 dunes
D. Reviewing the organization's risk appetite

Answer: B

NEW QUESTION 189
- (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 193
- (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 196
- (Exam Topic 1)
Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?

A. Relevance to the business process
B. Regulatory compliance requirements
C. Cost-benefit analysis
D. Comparison against best practice

Answer: B

NEW QUESTION 199
- (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 201
- (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 202
- (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 204
- (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 206
- (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 209
- (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 211
- (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 215
- (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 220
- (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 221
- (Exam Topic 2)
Which of the following should be of GREATEST concern to a risk practitioner when determining the effectiveness of IT controls?

A. Configuration updates do not follow formal change control.
B. Operational staff perform control self-assessments.
C. Controls are selected without a formal cost-benefit
D. analysis-Management reviews security policies once every two years.

Answer: A

NEW QUESTION 224
- (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 229
- (Exam Topic 2)
Whose risk tolerance matters MOST when making a risk decision?

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

Answer: C

NEW QUESTION 230
- (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 233
- (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 236
- (Exam Topic 2)
Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

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

Answer: C

NEW QUESTION 237
- (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 238
- (Exam Topic 2)
Which of the following will BEST help an organization evaluate the control environment of several third-party vendors?

A. Review vendors' internal risk assessments covering key risk and controls.
B. Obtain independent control reports from high-risk vendors.
C. Review vendors performance metrics on quality and delivery of processes.
D. Obtain vendor references from third parties.

Answer: B

NEW QUESTION 241
- (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 245

- (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 247
- (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 252
- (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 256
- (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 261
- (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 262
- (Exam Topic 2)
Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?

A. Enhance the security awareness program.
B. Increase the frequency of incident reporting.
C. Purchase cyber insurance from a third party.
D. Conduct a control assessment.

Answer: D

NEW QUESTION 265
- (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 268
- (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 270
- (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 271
- (Exam Topic 2)
The GREATEST concern when maintaining a risk register is that:

A. impacts are recorded in qualitative terms.
B. executive management does not perform periodic reviews.
C. IT risk is not linked with IT assets.
D. significant changes in risk factors are excluded.

Answer: D

NEW QUESTION 274
- (Exam Topic 2)
A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?

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

Answer: B

NEW QUESTION 277
- (Exam Topic 2)
An organization has raised the risk appetite for technology risk. The MOST likely result would be:

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

Answer: D

NEW QUESTION 279
- (Exam Topic 2)
Which of the following BEST helps to identify significant events that could impact an organization? Vulnerability analysis

A. Control analysis
B. Scenario analysis
C. Heat map analysis

Answer: C

NEW QUESTION 280
- (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 281
- (Exam Topic 2)
Which of the following is the MOST effective way to integrate risk and compliance management?

A. Embedding risk management into compliance decision-making
B. Designing corrective actions to improve risk response capabilities
C. Embedding risk management into processes that are aligned with business drivers
D. Conducting regular self-assessments to verify compliance

Answer: C

NEW QUESTION 285
- (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 286
- (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 291
- (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 292
- (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 295
- (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 297
- (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 300
- (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 304
- (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 306
- (Exam Topic 2)
IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

A. the cost associated with each control.
B. historical risk assessments.
C. key risk indicators (KRIs).
D. information from the risk register.

Answer: D

NEW QUESTION 308
- (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 309
- (Exam Topic 2)
Which of the following is the BEST evidence that a user account has been properly authorized?

A. An email from the user accepting the account
B. Notification from human resources that the account is active
C. User privileges matching the request form
D. Formal approval of the account by the user's manager

Answer: C

NEW QUESTION 314
- (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 317
- (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 10 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 318
- (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 321
- (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 324
- (Exam Topic 2)
Which of the following would be MOST helpful to a risk owner when making risk-aware decisions?

A. Risk exposure expressed in business terms
B. Recommendations for risk response options
C. Resource requirements for risk responses
D. List of business areas affected by the risk

Answer: A

NEW QUESTION 329
- (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 331
- (Exam Topic 2)
When updating a risk register with the results of an IT risk assessment, the risk practitioner should log:

A. high impact scenarios.
B. high likelihood scenarios.
C. treated risk scenarios.
D. known risk scenarios.

Answer: D

NEW QUESTION 335
- (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 338
- (Exam Topic 2)

Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?

A. Establishing a risk management committee
B. Updating the organization's risk register to reflect the new threat
C. Communicating the results of the threat impact analysis
D. Establishing metrics to assess the effectiveness of the responses

Answer: C

NEW QUESTION 343
- (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 346
- (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 350
- (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 353
- (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 354
- (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 356
- (Exam Topic 2)
Which of the following is the MOST effective way to integrate business risk management with IT operations?

A. Perform periodic IT control self-assessments.
B. Require a risk assessment with change requests.
C. Provide security awareness training.
D. Perform periodic risk assessments.

Answer: D

NEW QUESTION 358
- (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 359
- (Exam Topic 2)
An organization has completed a project to implement encryption on all databases that host customer data. Which of the following elements of the risk register should be updated the reflect this change?

A. Risk likelihood
B. Inherent risk
C. Risk appetite
D. Risk tolerance

Answer: B

NEW QUESTION 364
- (Exam Topic 2)
Which of the following is MOST effective in continuous risk management process improvement?

A. Periodic assessments
B. Change management
C. Awareness training
D. Policy updates

Answer: C

NEW QUESTION 366
- (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 371
- (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 376
- (Exam Topic 2)
Which of the following will BEST help in communicating strategic risk priorities?

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

Answer: D

NEW QUESTION 378
- (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 382
- (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 384
- (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 385
- (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 388
- (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 392
- (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 owne
B. Control owners approve control changes.
C. End-user acceptance testing has been conducte
D. Performance information in the log is encrypte

Answer: D

NEW QUESTION 397
- (Exam Topic 2)
During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

A. Include the new risk scenario in the current risk assessment.

B. Postpone the risk assessment until controls are identified.
C. Request the risk scenario be removed from the register.
D. Exclude the new risk scenario from the current risk assessment

Answer: A

NEW QUESTION 399
- (Exam Topic 2)
Which of the following criteria is MOST important when developing a response to an attack that would compromise data?

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

Answer: D

NEW QUESTION 400
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CRISC Practice Exam Features:

* CRISC Questions and Answers Updated Frequently

* CRISC Practice Questions Verified by Expert Senior Certified Staff

* CRISC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

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

100% Actual & Verified — Instant Download, Please Click
Order The CRISC Practice Test Here