Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

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)
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)
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 4
- (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 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)
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?

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

Answer: B

NEW QUESTION 8
- (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 9
- (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 10
- (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)
Which of the following is the MOST effective key performance indicator (KPI) for change management?

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

Answer: C

NEW QUESTION 15
- (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 17
- (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 19

- (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 22
- (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 25
- (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 29
- (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 31
- (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 34
- (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 36
- (Exam Topic 1)
Which of the following risk management practices BEST facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register?

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

Answer: D

NEW QUESTION 41
- (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 44
- (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 47
- (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 50
- (Exam Topic 1)
A risk practitioner is organizing a training session lo communicate risk assessment methodologies to ensure a consistent risk view within the organization Which of the following i< 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 54
- (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 58
- (Exam Topic 1)
An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?

A. Invoke the disaster recovery plan during an incident.
B. Prepare a cost-benefit analysis of alternatives available
C. Implement redundant infrastructure for the application.
D. Reduce the recovery time by strengthening the response team.

Answer: C

NEW QUESTION 63
- (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 67
- (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 71
- (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 73
- (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 81
- (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 85
- (Exam Topic 1)
Which of the following is MOST important when developing key performance indicators (KPIs)?

A. Alignment to risk responses
B. Alignment to management reports
C. Alerts when risk thresholds are reached
D. Identification of trends

Answer: C

NEW QUESTION 86
- (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 91
- (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 96
- (Exam Topic 1)
Which of the following should be the PRIMARY consideration when assessing the automation of control monitoring?

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

Answer: D

NEW QUESTION 100
- (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 102
- (Exam Topic 1)
A key risk indicator (KRI) is reported to senior management on a periodic basis as exceeding thresholds, but each time senior management has decided to take no action to reduce the risk. Which of the following is the MOST likely reason for senior management's response?

A. The underlying data source for the KRI is using inaccurate data and needs to be corrected.
B. The KRI is not providing useful information and should be removed from the KRI inventory.
C. The KRI threshold needs to be revised to better align with the organization s risk appetite
D. Senior management does not understand the KRI and should undergo risk training.

Answer: C

NEW QUESTION 103
- (Exam Topic 1)
A global organization is considering the acquisition of a competitor. Senior management has requested a review of the overall risk profile from the targeted organization. Which of the following components of this review would provide the MOST useful information?

A. Risk appetite statement
B. Enterprise risk management framework
C. Risk management policies
D. Risk register

Answer: D

NEW QUESTION 107
- (Exam Topic 1)
Which of the following attributes of a key risk indicator (KRI) is MOST important?

A. Repeatable
B. Automated
C. Quantitative
D. Qualitative

Answer: A

NEW QUESTION 108
- (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 112
- (Exam Topic 1)
Which of the following is the MOST important characteristic of an effective risk management program?

A. Risk response plans are documented
B. Controls are mapped to key risk scenarios.
C. Key risk indicators are defined.
D. Risk ownership is assigned

Answer: D

NEW QUESTION 116
- (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 120
- (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 121
- (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 125
- (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 128
- (Exam Topic 1)
Which of the following roles is BEST suited to help a risk practitioner understand the impact of IT-related events on business objectives?

A. IT management
B. Internal audit
C. Process owners
D. Senior management

Answer:

C

NEW QUESTION 130
- (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 135
- (Exam Topic 1)
The risk associated with an asset before controls are applied can be expressed as:

A. a function of the likelihood and impact
B. the magnitude of an impact
C. a function of the cost and effectiveness of control.
D. the likelihood of a given threat

Answer: C

NEW QUESTION 138
- (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 139
- (Exam Topic 1)
Which of the following is the MOST important benefit of key risk indicators (KRIs)'

A. Assisting in continually optimizing risk governance
B. Enabling the documentation and analysis of trends
C. Ensuring compliance with regulatory requirements
D. Providing an early warning to take proactive actions

Answer: D

NEW QUESTION 141
- (Exam Topic 1)
A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

A. Identify changes in risk factors and initiate risk reviews.
B. Engage an external consultant to redesign the risk management process.
C. Outsource the process for updating the risk register.
D. Implement a process improvement and replace the old risk register.

Answer: A

NEW QUESTION 145
- (Exam Topic 1)
Which of the following would be a risk practitioner'$ BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

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

Answer: B

NEW QUESTION 148
- (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 151
- (Exam Topic 1)
Which of the following would be- MOST helpful to understand the impact of a new technology system on an organization's current risk profile?

A. Hire consultants specializing m the new technology.
B. Review existing risk mitigation controls.
C. Conduct a gap analysis.
D. Perform a risk assessment.

Answer: D

NEW QUESTION 153
- (Exam Topic 1)
The MAIN purpose of conducting a control self-assessment (CSA) is to:

A. gain a better understanding of the control effectiveness in the organization
B. gain a better understanding of the risk in the organization
C. adjust the controls prior to an external audit
D. reduce the dependency on external audits

Answer: A

NEW QUESTION 157
- (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 161
- (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 162
- (Exam Topic 1)
An organization has allowed its cyber risk insurance to lapse while seeking a new insurance provider. The risk practitioner should report to management that the risk has been:

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

Answer: C

NEW QUESTION 166
- (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 170
- (Exam Topic 1)

Which of the following is the BEST way to validate the results of a vulnerability assessment?

A. Perform a penetration test.
B. Review security logs.
C. Conduct a threat analysis.
D. Perform a root cause analysis.

Answer: A

NEW QUESTION 173
- (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 175
- (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 179
- (Exam Topic 1)
An organization has determined a risk scenario is outside the defined risk tolerance level. What should be the NEXT course of action?

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

Answer: D

NEW QUESTION 184
- (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 188
- (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 193
- (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 194
- (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 197
- (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 198
- (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 201
- (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 206
- (Exam Topic 1)
Which of the following is a PRIMARY benefit of engaging the risk owner during the risk assessment process?

A. Identification of controls gaps that may lead to noncompliance
B. Prioritization of risk action plans across departments
C. Early detection of emerging threats
D. Accurate measurement of loss impact

Answer: D

NEW QUESTION 210
- (Exam Topic 1)
Senior management has asked a risk practitioner to develop technical risk scenarios related to a recently
developed enterprise resource planning (ERP) system. These scenarios will be owned by the system manager. Which of the following would be the BEST method to use when developing the scenarios?

A. Cause-and-effect diagram
B. Delphi technique
C. Bottom-up approach
D. Top-down approach

Answer: A

NEW QUESTION 215
- (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 216
- (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 220
- (Exam Topic 1)
A risk practitioners PRIMARY focus when validating a risk response action plan should be that risk response:

A. reduces risk to an acceptable level
B. quantifies risk impact
C. aligns with business strategy
D. advances business objectives.

Answer: A

NEW QUESTION 223
- (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 226
- (Exam Topic 1)
Which of the following is MOST important to communicate to senior management during the initial implementation of a risk management program?

A. Regulatory compliance
B. Risk ownership
C. Best practices
D. Desired risk level

Answer: A

NEW QUESTION 231
- (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 235
- (Exam Topic 1)
Which of the following should be management's PRIMARY consideration when approving risk response action plans?

A. Ability of the action plans to address multiple risk scenarios
B. Ease of implementing the risk treatment solution
C. Changes in residual risk after implementing the plans
D. Prioritization for implementing the action plans

Answer: D

NEW QUESTION 237
- (Exam Topic 1)
Which of the following is the MOST important factor affecting risk management in an organization?

A. The risk manager's expertise
B. Regulatory requirements
C. Board of directors' expertise

D. The organization's culture

Answer: B

NEW QUESTION 241
- (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 243
- (Exam Topic 1)
A review of an organization s controls has determined its data loss prevention {DLP) system is currently failing to detect outgoing emails containing credit card data. Which of the following would be MOST impacted?

A. Key risk indicators (KRls)
B. Inherent risk
C. Residual risk
D. Risk appetite

Answer: C

NEW QUESTION 244
- (Exam Topic 1)
Management has noticed storage costs have increased exponentially over the last 10 years because most users do not delete their emails. Which of the following can BEST alleviate this issue while not sacrificing security?

A. Implementing record retention tools and techniques
B. Establishing e-discovery and data loss prevention (DLP)
C. Sending notifications when near storage quota
D. Implementing a bring your own device 1BVOD) policy

Answer: A

NEW QUESTION 249
- (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 251
- (Exam Topic 1)
A risk practitioner observes that hardware failure incidents have been increasing over the last few months. However, due to built-in redundancy and fault-tolerant architecture, there have been no interruptions to business operations. The risk practitioner should conclude that:

A. a root cause analysis is required
B. controls are effective for ensuring continuity
C. hardware needs to be upgraded
D. no action is required as there was no impact

Answer: A

NEW QUESTION 254
- (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 257

- (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 258
- (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 260
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is aligned to business requirements?

A. Total cost to support the policy
B. Number of exceptions to the policy
C. Total cost of policy breaches
D. Number of inquiries regarding the policy

Answer: C

NEW QUESTION 265
- (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 268
- (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 273
- (Exam Topic 2)
An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:

A. identifying risk scenarios.
B. determining the risk strategy.
C. calculating impact and likelihood.
D. completing the controls catalog.

Answer: A

NEW QUESTION 274
- (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 276
- (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 277
- (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 278
- (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 281
- (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 284
- (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 285
- (Exam Topic 2)
Which of the following is MOST important to review when determining whether a potential IT service provider s control environment is effective?

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

Answer: A

NEW QUESTION 290
- (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 292
- (Exam Topic 2)
A bank wants to send a critical payment order via email to one of its offshore branches. Which of the following is the BEST way to ensure the message reaches the intended recipient without alteration?

A. Add a digital certificate
B. Apply multi-factor authentication
C. Add a hash to the message
D. Add a secret key

Answer: C

NEW QUESTION 295
- (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 300
- (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 302
- (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 303
- (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 304
- (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 309
- (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 310
- (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 313
- (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 317
- (Exam Topic 2)
Who should be responsible for implementing and maintaining security controls?

A. End user
B. Internal auditor
C. Data owner
D. Data custodian

Answer: D

NEW QUESTION 322
- (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 327
- (Exam Topic 2)
A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

A. strategy.
B. profile.
C. process.
D. map.

Answer: A

NEW QUESTION 332
- (Exam Topic 2)
Deviation from a mitigation action plan's completion date should be determined by which of the following?

A. Change management as determined by a change control board
B. Benchmarking analysis with similar completed projects
C. Project governance criteria as determined by the project office
D. The risk owner as determined by risk management processes

Answer: D

NEW QUESTION 337
- (Exam Topic 2)
An organization has identified that terminated employee accounts are not disabled or deleted within the time required by corporate policy. Unsure of the reason,

the organization has decided to monitor the situation for three months to obtain more information. As a result of this decision, the risk has been:

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

Answer: B

NEW QUESTION 342
- (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 343
- (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 348
- (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 350
- (Exam Topic 2)
An IT license audit has revealed that there are several unlicensed copies of co be to:

A. immediately uninstall the unlicensed software from the laptops
B. centralize administration rights on laptops so that installations are controlled
C. report the issue to management so appropriate action can be taken.
D. procure the requisite licenses for the software to minimize business impact.

Answer: B

NEW QUESTION 353
- (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 357
- (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 361
- (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 363
- (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 368
- (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 371
- (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 376
- (Exam Topic 2)
Which of the following is a KEY responsibility of the second line of defense?

A. Implementing control activities
B. Monitoring control effectiveness
C. Conducting control self-assessments
D. Owning risk scenarios

Answer: B

NEW QUESTION 380
- (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 381
- (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 385
- (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 388
- (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 391
- (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 396
- (Exam Topic 2)
Which of the following is MOST important when developing risk scenarios?

A. Reviewing business impact analysis (BIA)
B. Collaborating with IT audit
C. Conducting vulnerability assessments
D. Obtaining input from key stakeholders

Answer: D

NEW QUESTION 401
- (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 405
- (Exam Topic 2)
A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (Pll). 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 406
- (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 410
- (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 412
- (Exam Topic 2)
Which of The following is the PRIMARY consideration when establishing an organization's risk management methodology?

A. Business context
B. Risk tolerance level
C. Resource requirements
D. Benchmarking information

Answer: A

NEW QUESTION 414
- (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 416
- (Exam Topic 2)
The BEST way to improve a risk register is to ensure the register:

A. is updated based upon significant events.
B. documents possible countermeasures.
C. contains the risk assessment completion date.
D. is regularly audited.

Answer: D

NEW QUESTION 421
- (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 423
- (Exam Topic 2)
A risk practitioner learns that the organization s industry is experiencing a trend of rising security incidents. Which of the following is the BEST course of action?

A. Evaluate the relevance of the evolving threats.
B. Review past internal audit results.
C. Respond to organizational security threats.
D. Research industry published studies.

Answer: A

NEW QUESTION 424
- (Exam Topic 2)
An IT operations team implements disaster recovery controls based on decisions from application owners regarding the level of resiliency needed. Who is the risk owner in this scenario?

A. Business resilience manager

B. Disaster recovery team lead
C. Application owner
D. IT operations manager

Answer: C

NEW QUESTION 425
- (Exam Topic 2)
An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

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

Answer: B

NEW QUESTION 428
- (Exam Topic 2)
A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

A. Recommend avoiding the risk.
B. Validate the risk response with internal audit.
C. Update the risk register.
D. Evaluate outsourcing the process.

Answer: B

NEW QUESTION 432
- (Exam Topic 2)
To help ensure all applicable risk scenarios are incorporated into the risk register, it is MOST important to review the:

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

Answer: C

NEW QUESTION 433
- (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 438
- (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 440
- (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 444
- (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 447
- (Exam Topic 2)
Due to a change in business processes, an identified risk scenario no longer requires mitigation. Which of the following is the MOST important reason the risk should remain in the risk register?

A. To support regulatory requirements
B. To prevent the risk scenario in the current environment
C. To monitor for potential changes to the risk scenario
D. To track historical risk assessment results

Answer: D

NEW QUESTION 448
- (Exam Topic 2)
From a risk management perspective, which of the following is the PRIMARY benefit of using automated system configuration validation tools?

A. Residual risk is reduced.
B. Staff costs are reduced.
C. Operational costs are reduced.
D. Inherent risk is reduced.

Answer: A

NEW QUESTION 450
- (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 (B1A)
C. Control catalog
D. Risk register

Answer: D

NEW QUESTION 452
- (Exam Topic 2)
The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

A. availability of fault tolerant software.
B. strategic plan for business growth.
C. vulnerability scan results of critical systems.
D. redundancy of technical infrastructure.

Answer: D

NEW QUESTION 453
- (Exam Topic 2)
A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?

A. Recommend allowing the new usage based on prior approval.
B. Request a new third-party review.
C. Request revalidation of the original use case.
D. Assess the risk associated with the new use case.

Answer: D

NEW QUESTION 455
- (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 460
- (Exam Topic 2)
The PRIMARY purpose of IT control status reporting is to:

A. ensure compliance with IT governance strategy.
B. assist internal audit in evaluating and initiating remediation efforts.
C. benchmark IT controls with Industry standards.
D. facilitate the comparison of the current and desired states.

Answer: D

NEW QUESTION 465
- (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 470
- (Exam Topic 2)
The MOST important reason to aggregate results from multiple risk assessments on interdependent information systems is to:

A. establish overall impact to the organization
B. efficiently manage the scope of the assignment
C. identify critical information systems
D. facilitate communication to senior management

Answer: A

NEW QUESTION 475
.....

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