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)
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 4
- (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 5
- (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 6
- (Exam Topic 1)
Which of the following is the BEST method to identify unnecessary controls?

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

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
Periodically reviewing and updating a risk register with details on identified risk factors PRIMARILY helps to:

A. minimize the number of risk scenarios for risk assessment.
B. aggregate risk scenarios identified across different business units.
C. build a threat profile of the organization for management review.
D. provide a current reference to stakeholders for risk-based decisions.

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
A contract associated with a cloud service provider MUST include:

A. ownership of responsibilities.
B. a business recovery plan.
C. provision for source code escrow.
D. the providers financial statements.

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
The analysis of which of the following will BEST help validate whether suspicious network activity is malicious?

A. Logs and system events
B. Intrusion detection system (IDS) rules
C. Vulnerability assessment reports
D. Penetration test reports

Answer: B

NEW QUESTION 10
- (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 10
- (Exam Topic 1)
Which of the following is the MAIN reason to continuously monitor IT-related risk?

A. To redefine the risk appetite and risk tolerance levels based on changes in risk factors
B. To update the risk register to reflect changes in levels of identified and new IT-related risk
C. To ensure risk levels are within acceptable limits of the organization's risk appetite and risk tolerance
D. To help identify root causes of incidents and recommend suitable long-term solutions

Answer: C

NEW QUESTION 13
- (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 18
- (Exam Topic 1)
Which of the following is the MOST important element of a successful risk awareness training program?

A. Customizing content for the audience
B. Providing incentives to participants
C. Mapping to a recognized standard
D. Providing metrics for measurement

Answer: A

NEW QUESTION 21
- (Exam Topic 1)
IT risk assessments can BEST be used by management:

A. for compliance with laws and regulations
B. as a basis for cost-benefit analysis.

C. as input foe decision-making
D. to measure organizational success.

Answer: C

NEW QUESTION 22
- (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 26
- (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 27
- (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 30
- (Exam Topic 1)
Which of the following would BEST provide early warning of a high-risk condition?

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

Answer: C

NEW QUESTION 33
- (Exam Topic 1)
A risk assessment has identified that an organization may not be in compliance with industry regulations. The BEST course of action would be to:

A. conduct a gap analysis against compliance criteria.
B. identify necessary controls to ensure compliance.
C. modify internal assurance activities to include control validation.
D. collaborate with management to meet compliance requirements.

Answer: A

NEW QUESTION 37
- (Exam Topic 1)
Which of the following is the BEST key performance indicator (KPI) to measure the maturity of an organization's security incident handling process?

A. The number of security incidents escalated to senior management
B. The number of resolved security incidents
C. The number of newly identified security incidents
D. The number of recurring security incidents

Answer: B

NEW QUESTION 39
- (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 40
- (Exam Topic 1)
Which of the following will BEST quantify the risk associated with malicious users in an organization?

A. Business impact analysis
B. Risk analysis
C. Threat risk assessment
D. Vulnerability assessment

Answer: A

NEW QUESTION 43
- (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 47
- (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 51
- (Exam Topic 1)
Which of the following is MOST important to understand when determining an appropriate risk assessment approach?

A. Complexity of the IT infrastructure
B. Value of information assets
C. Management culture
D. Threats and vulnerabilities

Answer: A

NEW QUESTION 56
- (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 60
- (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 63
- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 66
- (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 67
- (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 69
- (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 70
- (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 73
- (Exam Topic 1)
After a risk has been identified, who is in the BEST position to select the appropriate risk treatment option?

A. The risk practitioner
B. The business process owner
C. The risk owner
D. The control owner

Answer: C

NEW QUESTION 76
- (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 79
- (Exam Topic 1)
An organization wants to assess the maturity of its internal control environment. The FIRST step should be to:

A. validate control process execution.
B. determine if controls are effective.
C. identify key process owners.
D. conduct a baseline assessment.

Answer: C

NEW QUESTION 81
- (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 86
- (Exam Topic 1)
Which of the following IT controls is MOST useful in mitigating the risk associated with inaccurate data?

A. Encrypted storage of data
B. Links to source data
C. Audit trails for updates and deletions
D. Check totals on data records and data fields

Answer: C

NEW QUESTION 90
- (Exam Topic 1)
Which of the following would MOST effectively enable a business operations manager to identify events exceeding risk thresholds?

A. Continuous monitoring
B. A control self-assessment
C. Transaction logging
D. Benchmarking against peers

Answer: A

NEW QUESTION 91
- (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 94
- (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 98
- (Exam Topic 1)
Which of the following elements of a risk register is MOST likely to change as a result of change in management's risk appetite?

A. Key risk indicator (KRI) thresholds
B. Inherent risk
C. Risk likelihood and impact
D. Risk velocity

Answer:

A

NEW QUESTION 102
- (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 104
- (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 109
- (Exam Topic 1)
Which of the following roles would provide the MOST important input when identifying IT risk scenarios?

A. Information security managers
B. Internal auditors
C. Business process owners
D. Operational risk managers

Answer: C

NEW QUESTION 111
- (Exam Topic 1)
Which of the following is the PRIMARY reason to perform ongoing risk assessments?

A. Emerging risk must be continuously reported to management.
B. New system vulnerabilities emerge at frequent intervals.
C. The risk environment is subject to change.
D. The information security budget must be justified.

Answer: C

NEW QUESTION 116
- (Exam Topic 1)
IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would
be MOST helpful?

A. IT risk register
B. List of key risk indicators
C. Internal audit reports
D. List of approved projects

Answer: A

NEW QUESTION 117
- (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 118
- (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 121
- (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 124
- (Exam Topic 1)
A risk assessment has identified that departments have installed their own WiFi access points on the enterprise network. Which of the following would be MOST important to include in a report to senior management?

A. The network security policy
B. Potential business impact
C. The WiFi access point configuration
D. Planned remediation actions

Answer: B

NEW QUESTION 126
- (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 129
- (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 132
- (Exam Topic 1)
A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

A. IT system owner
B. Chief financial officer
C. Chief risk officer
D. Business process owner

Answer: D

NEW QUESTION 133
- (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 135

- (Exam Topic 1)
Which of the following would provide the BEST guidance when selecting an appropriate risk treatment plan?

A. Risk mitigation budget
B. Business Impact analysis
C. Cost-benefit analysis
D. Return on investment

Answer: B

NEW QUESTION 140
- (Exam Topic 1)
It is MOST appropriate for changes to be promoted to production after they are;

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

Answer: B

NEW QUESTION 141
- (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 145
- (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 149
- (Exam Topic 1)
A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

A. better understands the system architecture.
B. is more objective than risk management.
C. can balance technical and business risk.
D. can make better informed business decisions.

Answer: D

NEW QUESTION 152
- (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 154
- (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 158
- (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 162
- (Exam Topic 1)
Which of the following would be MOST useful when measuring the progress of a risk response action plan?

A. Percentage of mitigated risk scenarios
B. Annual loss expectancy (ALE) changes
C. Resource expenditure against budget
D. An up-to-date risk register

Answer: D

NEW QUESTION 167
- (Exam Topic 1)
Which of the following activities would BEST contribute to promoting an organization-wide risk-aware culture?

A. Performing a benchmark analysis and evaluating gaps
B. Conducting risk assessments and implementing controls
C. Communicating components of risk and their acceptable levels
D. Participating in peer reviews and implementing best practices

Answer: C

NEW QUESTION 168
- (Exam Topic 1)
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

A. Ensure compliance.
B. Identify trends.
C. Promote a risk-aware culture.
D. Optimize resources needed for controls

Answer: B

NEW QUESTION 172
- (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 175
- (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 176
- (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 181
- (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 183
- (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 187
- (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 190
- (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 195
- (Exam Topic 2)
To mitigate the risk of using a spreadsheet to analyze financial data, IT has engaged a third-party vendor to deploy a standard application to automate the process. Which of the following parties should own the risk associated with calculation errors?

A. business owner
B. IT department
C. Risk manager
D. Third-party provider

Answer: D

NEW QUESTION 196
- (Exam Topic 2)
Which of the following conditions presents the GREATEST risk to an application?

A. Application controls are manual.
B. Application development is outsourced.
C. Source code is escrowed.
D. Developers have access to production environment.

Answer: D

NEW QUESTION 199
- (Exam Topic 2)
A maturity model will BEST indicate:

A. confidentiality and integrity.
B. effectiveness and efficiency.
C. availability and reliability.

D. certification and accreditation.

Answer: B

NEW QUESTION 200
- (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 201
- (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 205
- (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 206
- (Exam Topic 2)
Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

A. Align business objectives with risk appetite.
B. Enable risk-based decision making.
C. Design and implement risk response action plans.
D. Update risk responses in the risk register

Answer: B

NEW QUESTION 211
- (Exam Topic 2)
Which of the following BEST indicates whether security awareness training is effective?

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

Answer: B

NEW QUESTION 212
- (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 214
- (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 216
- (Exam Topic 2)
The PRIMARY benefit associated with key risk indicators (KRIs) is that they

A. help an organization identify emerging threats.
B. benchmark the organization's risk profile.
C. identify trends in the organization's vulnerabilities.
D. enable ongoing monitoring of emerging risk.

Answer: A

NEW QUESTION 217
- (Exam Topic 2)
A risk practitioner notices that a particular key risk indicator (KRI) has remained below its established trigger point for an extended period of time. Which of the following should be done FIRST?

A. Recommend a re-evaluation of the current threshold of the KRI.
B. Notify management that KRIs are being effectively managed.
C. Update the risk rating associated with the KRI In the risk register.
D. Update the risk tolerance and risk appetite to better align to the KRI.

Answer: A

NEW QUESTION 218
- (Exam Topic 2)
Quantifying the value of a single asset helps the organization to understand the:

A. overall effectiveness of risk management
B. consequences of risk materializing
C. necessity of developing a risk strategy,
D. organization s risk threshold.

Answer: B

NEW QUESTION 219
- (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 223
- (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 224
- (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 229

- (Exam Topic 2)
Which of the following BEST measures the efficiency of an incident response process?

A. Number of incidents escalated to management
B. Average time between changes and updating of escalation matrix
C. Average gap between actual and agreed response times
D. Number of incidents lacking responses

Answer: C

NEW QUESTION 230
- (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 234
- (Exam Topic 2)
When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

A. An anal/sis of the security logs that illustrate the sequence of events
B. An analysis of the impact of similar attacks in other organizations
C. A business case for implementing stronger logical access controls
D. A justification of corrective action taken

Answer: A

NEW QUESTION 236
- (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 241
- (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 242
- (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 243
- (Exam Topic 2)
The PRIMARY objective of The board of directors periodically reviewing the risk profile is to help ensure:

A. the risk strategy is appropriate
B. KRIs and KPIs are aligned
C. performance of controls is adequate
D. the risk monitoring process has been established

Answer: B

NEW QUESTION 247

- (Exam Topic 2)
The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

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

Answer: A

NEW QUESTION 251
- (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 252
- (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 256
- (Exam Topic 2)
A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

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

Answer: C

NEW QUESTION 259
- (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 264
- (Exam Topic 2)
Which of the following BEST promotes commitment to controls?

A. Assigning control ownership
B. Assigning appropriate resources
C. Assigning a quality control review
D. Performing regular independent control reviews

Answer: A

NEW QUESTION 266
- (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 269
- (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 272
- (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 (KRls).
D. information from the risk register.

Answer: D

NEW QUESTION 277
- (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 282
- (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 284
- (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 285
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

A. Percentage of business users completing risk training
B. Percentage of high-risk scenarios for which risk action plans have been developed
C. Number of key risk indicators (KRIs) defined
D. Time between when IT risk scenarios are identified and the enterprise's response

Answer: C

NEW QUESTION 289
- (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 293
- (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 295
- (Exam Topic 2)
What should be the PRIMARY objective for a risk practitioner performing a post-implementation review of an IT risk mitigation project?

A. Documenting project lessons learned
B. Validating the risk mitigation project has been completed
C. Confirming that the project budget was not exceeded
D. Verifying that the risk level has been lowered

Answer: A

NEW QUESTION 298
- (Exam Topic 2)
An internal audit report reveals that not all IT application databases have encryption in place. Which of the following information would be MOST important for assessing the risk impact?

A. The number of users who can access sensitive data
B. A list of unencrypted databases which contain sensitive data
C. The reason some databases have not been encrypted
D. The cost required to enforce encryption

Answer: B

NEW QUESTION 302
- (Exam Topic 2)
Which of the following should be included in a risk assessment report to BEST facilitate senior management's understanding of the results?

A. Benchmarking parameters likely to affect the results
B. Tools and techniques used by risk owners to perform the assessments
C. A risk heat map with a summary of risk identified and assessed
D. The possible impact of internal and external risk factors on the assessment results

Answer: C

NEW QUESTION 307
- (Exam Topic 2)
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 310
- (Exam Topic 2)
Sensitive data has been lost after an employee inadvertently removed a file from the premises, in violation of organizational policy. Which of the following controls MOST likely failed?

A. Background checks
B. Awareness training
C. User access
D. Policy management

Answer: C

NEW QUESTION 312
- (Exam Topic 2)
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 316
- (Exam Topic 2)
A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

A. Ask the business to make a budget request to remediate the problem.
B. Build a business case to remediate the fix.
C. Research the types of attacks the threat can present.
D. Determine the impact of the missing threat.

Answer: D

NEW QUESTION 320
- (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 324
- (Exam Topic 2)
A software developer has administrative access to a production application. Which of the following should be of GREATEST concern to a risk practitioner?

A. The administrative access does not allow for activity log monitoring.
B. The administrative access does not follow password management protocols.
C. The administrative access represents a deviation from corporate policy.
D. The administrative access represents a segregation of duties conflict.

Answer: D

NEW QUESTION 328
- (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 331
- (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 332
- (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 335

- (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 340
- (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 341
- (Exam Topic 2)
Which of the following BEST indicates effective information security incident management?

A. Monthly trend of information security-related incidents
B. Average time to identify critical information security incidents
C. Frequency of information security incident response plan testing
D. Percentage of high risk security incidents

Answer: B

NEW QUESTION 345
- (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 350
- (Exam Topic 2)
Which of the following is the BEST way to support communication of emerging risk?

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

Answer: D

NEW QUESTION 351
- (Exam Topic 2)
Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

A. Risk tolerance
B. Risk appetite
C. Risk awareness
D. Risk policy

Answer: A

NEW QUESTION 356
......