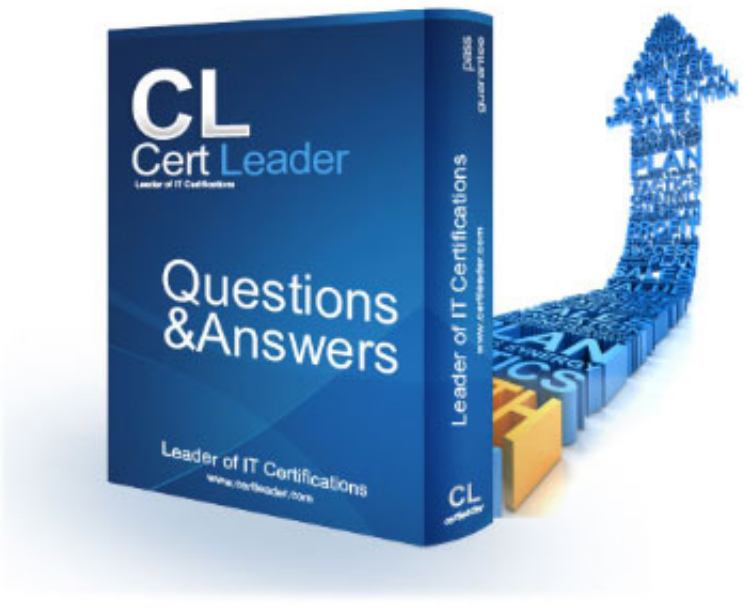
CRISC Dumps

Certified in Risk and Information Systems Control

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



NEW QUESTION 1
- (Exam Topic 1)
A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

A. Obtain the risk owner's approval.
B. Record the risk as accepted m the risk register.
C. Inform senior management.
D. update the risk response plan.

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
Which of the following BEST provides an early warning that network access of terminated employees is not being revoked in accordance with the service level agreement (SLA)?

A. Updating multi-factor authentication
B. Monitoring key access control performance indicators
C. Analyzing access control logs for suspicious activity
D. Revising the service level agreement (SLA)

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
A risk practitioner is assisting with the preparation of a report on the organization s disaster recovery (DR) capabilities. Which information would have the MOST impact on the overall recovery profile?

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

Answer: D

NEW QUESTION 4
- (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 5
- (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 6
- (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 7
- (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 8
- (Exam Topic 1)
In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

A. two-factor authentication.
B. continuous data backup controls.
C. encryption for data at rest.
D. encryption for data in motion.

Answer: B

NEW QUESTION 9
- (Exam Topic 1)
An organization delegates its data processing to the internal IT team to manage information through its applications. Which of the following is the role of the internal IT team in this situation?

A. Data controllers
B. Data processors
C. Data custodians
D. Data owners

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
Which of the following should be the risk practitioner s PRIMARY focus when determining whether controls are adequate to mitigate risk?

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

Answer: C

NEW QUESTION 10
- (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 11
- (Exam Topic 1)
A trusted third party service provider has determined that the risk of a client's systems being hacked is low. Which of the following would be the client's BEST course of action?

A. Perform their own risk assessment
B. Implement additional controls to address the risk.
C. Accept the risk based on the third party's risk assessment
D. Perform an independent audit of the third party.

Answer: C

NEW QUESTION 14
- (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 18
- (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 23
- (Exam Topic 1)
A web-based service provider with a low risk appetite for system outages is reviewing its current risk profile for online security. Which of the following observations would be MOST relevant to escalate to senior management?

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

Answer: A

NEW QUESTION 27
- (Exam Topic 1)
While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

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

Answer: A

NEW QUESTION 29
- (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 32
- (Exam Topic 1)
Calculation of the recovery time objective (RTO) is necessary to determine the:

A. time required to restore files.
B. point of synchronization
C. priority of restoration.
D. annual loss expectancy (ALE).

Answer: A

NEW QUESTION 37
- (Exam Topic 1)
Which of the following changes would be reflected in an organization's risk profile after the failure of a critical patch implementation?

A. Risk tolerance is decreased.
B. Residual risk is increased.
C. Inherent risk is increased.
D. Risk appetite is decreased

Answer: D

NEW QUESTION 41
- (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 42
- (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 45
- (Exam Topic 1)
An organization has outsourced its IT security operations to a third party. Who is ULTIMATELY accountable for the risk associated with the outsourced operations?

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

Answer: B

NEW QUESTION 47
- (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 50
- (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 54
- (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 59
- (Exam Topic 1)
A risk practitioner has observed that there is an increasing trend of users sending sensitive information by email without using encryption. Which of the following would be the MOST effective approach to mitigate the risk associated with data loss?

A. Implement a tool to create and distribute violation reports
B. Raise awareness of encryption requirements for sensitive data.
C. Block unencrypted outgoing emails which contain sensitive data.
D. Implement a progressive disciplinary process for email violations.

Answer: C

NEW QUESTION 60
- (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 63
- (Exam Topic 1)
Which of the following is the GREATEST benefit of incorporating IT risk scenarios into the corporate risk register?

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

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
The number of tickets to rework application code has significantly exceeded the established threshold. Which of the following would be the risk practitioner s BEST recommendation?

A. Perform a root cause analysis
B. Perform a code review
C. Implement version control software.
D. Implement training on coding best practices

Answer: A

NEW QUESTION 67
- (Exam Topic 1)
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 68
- (Exam Topic 1)
Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?

A. Assess the vulnerability management process.
B. Conduct a control serf-assessment.
C. Conduct a vulnerability assessment.
D. Reassess the inherent risk of the target.

Answer: C

NEW QUESTION 73
- (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 76
- (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 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)
Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

A. Key risk indicators
B. Risk scenarios
C. Business impact analysis
D. Threat analysis

Answer: B

NEW QUESTION 86
- (Exam Topic 1)
Which of the following is MOST useful when communicating risk to management?

A. Risk policy
B. Audit report
C. Risk map
D. Maturity model

Answer: A

NEW QUESTION 88
- (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 92
- (Exam Topic 1)
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

A. Sufficient resources are not assigned to IT development projects.
B. Customer support help desk staff does not have adequate training.
C. Email infrastructure does not have proper rollback plans.
D. The corporate email system does not identify and store phishing emails.

Answer: A

NEW QUESTION 96
- (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 97
- (Exam Topic 1)
When updating the risk register after a risk assessment, which of the following is MOST important to include?

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

Answer: C

NEW QUESTION 98
- (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 99
- (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 102
- (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 105
- (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 106
- (Exam Topic 1)
Which of the following will BEST mitigate the risk associated with IT and business misalignment?

A. Establishing business key performance indicators (KPIs)
B. Introducing an established framework for IT architecture
C. Establishing key risk indicators (KRIs)
D. Involving the business process owner in IT strategy

Answer: D

NEW QUESTION 111
- (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 113
- (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 115
- (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 116
- (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 118
- (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 121
- (Exam Topic 1)
The BEST reason to classify IT assets during a risk assessment is to determine the:

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

Answer: D

NEW QUESTION 126
- (Exam Topic 1)
When reviewing management's IT control self-assessments, a risk practitioner noted an ineffective control that links to several low residual risk scenarios. What should be the NEXT course of action?

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

Answer: D

NEW QUESTION 131
- (Exam Topic 1)
Which of the following is MOST critical when designing controls?

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

Answer: B

NEW QUESTION 134
- (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 138
- (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 139
- (Exam Topic 1)
During the risk assessment of an organization that processes credit cards, a number of existing controls have been found to be ineffective and do not meet industry standards. The overall control environment may still be effective if:

A. compensating controls are in place.
B. a control mitigation plan is in place.
C. risk management is effective.
D. residual risk is accepted.

Answer: A

NEW QUESTION 144
- (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 149
- (Exam Topic 1)
Which of the following should be the PRIMARY consideration when implementing controls for monitoring user activity logs?

A. Ensuring availability of resources for log analysis
B. Implementing log analysis tools to automate controls
C. Ensuring the control is proportional to the risk
D. Building correlations between logs collected from different sources

Answer: C

NEW QUESTION 152
- (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 154
- (Exam Topic 1)
Which of the following is the FIRST step in managing the security risk associated with wearable technology in the workplace?

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

Answer: A

NEW QUESTION 157
- (Exam Topic 1)
An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course

of action?

A. Report the observation to the chief risk officer (CRO).
B. Validate the adequacy of the implemented risk mitigation measures.
C. Update the risk register with the implemented risk mitigation actions.
D. Revert the implemented mitigation measures until approval is obtained

Answer: A

NEW QUESTION 160
- (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 162
- (Exam Topic 1)
In addition to the risk register, what should a risk practitioner review to develop an understanding of the organization's risk profile?

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

Answer: C

NEW QUESTION 166
- (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 167
- (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 172
- (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 175
- (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 176
- (Exam Topic 2)
Which of the following can be used to assign a monetary value to risk?

A. Annual loss expectancy (ALE)
B. Business impact analysis
C. Cost-benefit analysis
D. Inherent vulnerabilities

Answer: A

NEW QUESTION 177
- (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 180
- (Exam Topic 2)
Which of the following statements in an organization's current risk profile report is cause for further action by senior management?

A. Key performance indicator (KPI) trend data is incomplete.
B. New key risk indicators (KRIs) have been established.
C. Key performance indicators (KPIs) are outside of targets.
D. Key risk indicators (KRIs) are lagging.

Answer: C

NEW QUESTION 182
- (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 185
- (Exam Topic 2)
An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

A. Implement database activity and capacity monitoring.
B. Ensure the business is aware of the risk.
C. Ensure the enterprise has a process to detect such situations.
D. Consider providing additional system resources to this job.

Answer: B

NEW QUESTION 187
- (Exam Topic 2)
An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

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

Answer: A

NEW QUESTION 191
- (Exam Topic 2)
An organization's financial analysis department uses an in-house forecasting application for business projections. Who is responsible for defining access roles to protect the sensitive data within this application?

A. IT risk manager
B. IT system owner
C. Information security manager
D. Business owner

Answer: D

NEW QUESTION 193
- (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 195
- (Exam Topic 2)
When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:

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

Answer: B

NEW QUESTION 198
- (Exam Topic 2)
Which of the following is MOST important for an organization to have in place when developing a risk management framework?

A. A strategic approach to risk including an established risk appetite
B. A risk-based internal audit plan for the organization
C. A control function within the risk management team
D. An organization-wide risk awareness training program

Answer: A

NEW QUESTION 200
- (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 202
- (Exam Topic 2)
Which of the following would be a weakness in procedures for controlling the migration of changes to production libraries?

A. The programming project leader solely reviews test results before approving the transfer to production.
B. Test and production programs are in distinct libraries.
C. Only operations personnel are authorized to access production libraries.
D. A synchronized migration of executable and source code from the test environment to the production environment is allowed.

Answer: D

NEW QUESTION 204
- (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 206
- (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 207
- (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 211
- (Exam Topic 2)
Which of the following is the MOST effective way to integrate risk and compliance management?

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

Answer: C

NEW QUESTION 214
- (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 215
- (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 216
- (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 219
- (Exam Topic 2)
Implementing which of the following will BEST help ensure that systems comply with an established baseline before deployment?

A. Vulnerability scanning
B. Continuous monitoring and alerting
C. Configuration management
D. Access controls and active logging

Answer: C

NEW QUESTION 220
- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to consider when evaluating plans for changes to IT services?

A. Change testing schedule
B. Impact assessment of the change
C. Change communication plan
D. User acceptance testing (UAT)

Answer: D

NEW QUESTION 224
- (Exam Topic 2)
Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

A. An internal audit
B. Security operations center review
C. Internal penetration testing
D. A third-party audit

Answer: A

NEW QUESTION 227
- (Exam Topic 2)
Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?

A. Defining expectations in the enterprise risk policy
B. Increasing organizational resources to mitigate risks
C. Communicating external audit results
D. Avoiding risks that could materialize into substantial losses

Answer: D

NEW QUESTION 228
- (Exam Topic 2)
During the initial risk identification process for a business application, it is MOST important to include which of the following stakeholders?

A. Business process owners
B. Business process consumers
C. Application architecture team
D. Internal audit

Answer: A

NEW QUESTION 232
- (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 235
- (Exam Topic 2)
Which of the following would BEST enable mitigation of newly identified risk factors related to internet of Things (IoT)?

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

Answer: A

NEW QUESTION 237
- (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 242

- (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 247
- (Exam Topic 2)
An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

A. Review the risk identification process.
B. Inform the risk scenario owners.
C. Create a risk awareness communication plan.
D. Update the risk register.

Answer: A

NEW QUESTION 252
- (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 255
- (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 258
- (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 263
- (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 264
- (Exam Topic 2)
Which of the following is the MOST effective way to integrate business risk management with IT operations?

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

Answer: D

NEW QUESTION 269
- (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 273
- (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 278
- (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 282
- (Exam Topic 2)
Which of the following will BEST help in communicating strategic risk priorities?

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

Answer: D

NEW QUESTION 285
- (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 290
- (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 293
- (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 295
- (Exam Topic 2)
Which of the following will BEST help an organization select a recovery strategy for critical systems?

A. Review the business impact analysis.
B. Create a business continuity plan.
C. Analyze previous disaster recovery reports.
D. Conduct a root cause analysis.

Answer: A

NEW QUESTION 296
- (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 299
- (Exam Topic 2)
An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?

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

Answer: B

NEW QUESTION 301
- (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 303
- (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 307
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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