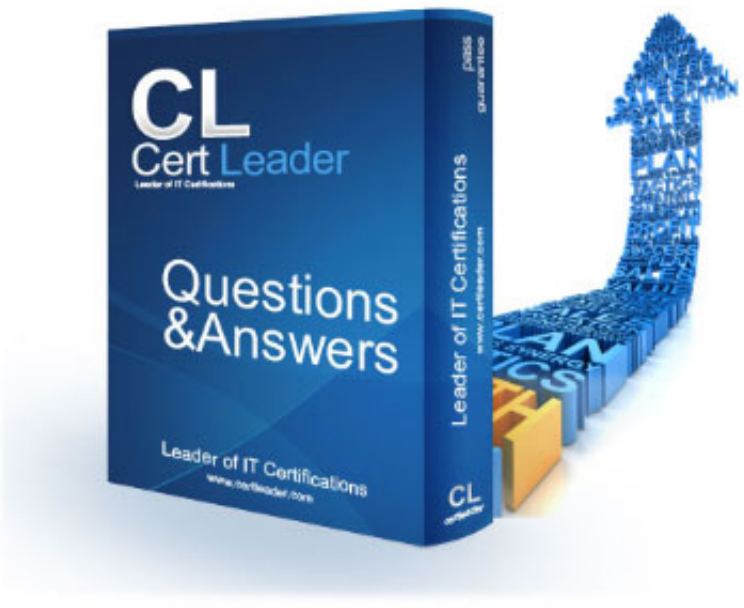
CRISC Dumps

Certified in Risk and Information Systems Control

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



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)
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 3
- (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 4
- (Exam Topic 1)
The PRIMARY objective of testing the effectiveness of a new control before implementation is to:

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

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

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

Answer: C

NEW QUESTION 6
- (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 7
- (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 8
- (Exam Topic 1)
Which of the following is the BEST way to identify changes to the risk landscape?

A. Internal audit reports
B. Access reviews
C. Threat modeling
D. Root cause analysis

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
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 10
- (Exam Topic 1)
Which of the following is the BEST indication of an improved risk-aware culture following the implementation of a security awareness training program for all employees?

A. A reduction in the number of help desk calls
B. An increase in the number of identified system flaws
C. A reduction in the number of user access resets
D. An increase in the number of incidents reported

Answer: B

NEW QUESTION 15
- (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 17
- (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 21
- (Exam Topic 1)

Which of the following is the MOST important data source for monitoring key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 23
- (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 24
- (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 27
- (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 30
- (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 31
- (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 33
- (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 38
- (Exam Topic 1)
To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:

A. require the vendor to sign a nondisclosure agreement
B. clearly define the project scope.
C. perform background checks on the vendor.
D. notify network administrators before testing

Answer: A

NEW QUESTION 39
- (Exam Topic 1)
Reviewing results from which of the following is the BEST way to identify information systems control deficiencies?

A. Vulnerability and threat analysis
B. Control remediation planning
C. User acceptance testing (UAT)
D. Control self-assessment (CSA)

Answer: D

NEW QUESTION 43
- (Exam Topic 1)
Whether the results of risk analyses should be presented in quantitative or qualitative terms should be based PRIMARILY on the:

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

Answer: A

NEW QUESTION 47
- (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 48
- (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 51
- (Exam Topic 1)
The MOST effective way to increase the likelihood that risk responses will be implemented is to:

A. create an action plan
B. assign ownership
C. review progress reports
D. perform regular audits.

Answer: B

NEW QUESTION 53
- (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 54
- (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 58
- (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 63
- (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 64
- (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 67
- (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 68
- (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 73
- (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 75
- (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 79
- (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 82
- (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 84
- (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 86
- (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 89
- (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 92
- (Exam Topic 1)
Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

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

Answer: B

NEW QUESTION 93
- (Exam Topic 1)
An unauthorized individual has socially engineered entry into an organization's secured physical premises. Which of the following is the BEST way to prevent future occurrences?

A. Employ security guards.
B. Conduct security awareness training.
C. Install security cameras.
D. Require security access badges.

Answer: B

NEW QUESTION 98
- (Exam Topic 1)
Which of the following is the MOST important consideration when sharing risk management updates with executive management?

A. Using an aggregated view of organizational risk
B. Ensuring relevance to organizational goals
C. Relying on key risk indicator (KRI) data Including
D. Trend analysis of risk metrics

Answer: B

NEW QUESTION 103
- (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 104
- (Exam Topic 1)
To implement the MOST effective monitoring of key risk indicators (KRIs), which of the following needs to be in place?

A. Threshold definition
B. Escalation procedures
C. Automated data feed
D. Controls monitoring

Answer: A

NEW QUESTION 105
- (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 106
- (Exam Topic 1)
Which of the following is the BEST way for a risk practitioner to help management prioritize risk response?

A. Align business objectives to the risk profile.
B. Assess risk against business objectives
C. Implement an organization-specific risk taxonomy.
D. Explain risk details to management.

Answer: B

NEW QUESTION 108
- (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 113
- (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 118
- (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 122
- (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 126
- (Exam Topic 1)
A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application. Who should have the authority to accept the associated risk?

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

Answer: C

NEW QUESTION 129
- (Exam Topic 1)
A risk practitioner is developing a set of bottom-up IT risk scenarios. The MOST important time to involve business stakeholders is when:

A. updating the risk register
B. documenting the risk scenarios.
C. validating the risk scenarios
D. identifying risk mitigation controls.

Answer: C

NEW QUESTION 133
- (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 is the BEST method for assessing control effectiveness?

A. Ad hoc control reporting
B. Control self-assessment
C. Continuous monitoring
D. Predictive analytics

Answer: C

NEW QUESTION 139
- (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 143
- (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 147
- (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 150
- (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 151
- (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 156
- (Exam Topic 1)
When determining which control deficiencies are most significant, which of the following would provide the MOST useful information?

A. Risk analysis results
B. Exception handling policy

C. Vulnerability assessment results
D. Benchmarking assessments

Answer: C

NEW QUESTION 158
- (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 163
- (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 (KRIs)
B. Inherent risk
C. Residual risk
D. Risk appetite

Answer: C

NEW QUESTION 167
- (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 169
- (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 173
- (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 177
- (Exam Topic 2)
Controls should be defined during the design phase of system development because:

A. it is more cost-effective to determine controls in the early design phase.
B. structured analysis techniques exclude identification of controls.
C. structured programming techniques require that controls be designed before coding begins.
D. technical specifications are defined during this phase.

Answer: D

NEW QUESTION 181
- (Exam Topic 2)

Who is PRIMARILY accountable for risk treatment decisions?

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

Answer: B

NEW QUESTION 184
- (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 190
- (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 194
- (Exam Topic 2)
Which of the following is MOST helpful in aligning IT risk with business objectives?

A. Introducing an approved IT governance framework
B. Integrating the results of top-down risk scenario analyses
C. Performing a business impact analysis (BIA)
D. Implementing a risk classification system

Answer: A

NEW QUESTION 199
- (Exam Topic 2)
Which of the following should be the PRIMARY objective of a risk awareness training program?

A. To enable risk-based decision making
B. To promote awareness of the risk governance function
C. To clarify fundamental risk management principles
D. To ensure sufficient resources are available

Answer: A

NEW QUESTION 202
- (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 204
- (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 209
- (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 210
- (Exam Topic 2)
Which of the following BEST indicates the efficiency of a process for granting access privileges?

A. Average time to grant access privileges
B. Number of changes in access granted to users
C. Average number of access privilege exceptions
D. Number and type of locked obsolete accounts

Answer: A

NEW QUESTION 213
- (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 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 216
- (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 218
- (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 223
- (Exam Topic 2)
An upward trend in which of the following metrics should be of MOST concern?

A. Number of business change management requests
B. Number of revisions to security policy
C. Number of security policy exceptions approved
D. Number of changes to firewall rules

Answer: C

NEW QUESTION 227
- (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 229
- (Exam Topic 2)
Which of the following is a detective control?

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

Answer: B

NEW QUESTION 232
- (Exam Topic 2)
A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?

A. Review the design of the machine learning model against control objectives.
B. Adopt the machine learning model as a replacement for current manual access reviews.
C. Ensure the model assists in meeting regulatory requirements for access controls.
D. Discourage the use of emerging technologies in key processes.

Answer: A

NEW QUESTION 236
- (Exam Topic 2)
Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?

A. A companion of risk assessment results to the desired state
B. A quantitative presentation of risk assessment results
C. An assessment of organizational maturity levels and readiness
D. A qualitative presentation of risk assessment results

Answer: D

NEW QUESTION 238
- (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 241
- (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 244
- (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 249
- (Exam Topic 2)
A risk practitioner is reporting on an increasing trend of ransomware attacks in the industry. Which of the following information is MOST important to include to enable an informed response decision by key stakeholders?

A. Methods of attack progression
B. Losses incurred by industry peers
C. Most recent antivirus scan reports
D. Potential impact of events

Answer: D

NEW QUESTION 252
- (Exam Topic 2)
The PRIMARY purpose of using control metrics is to evaluate the:

A. amount of risk reduced by compensating controls.
B. amount of risk present in the organization.
C. variance against objectives.
D. number of incidents.

Answer: C

NEW QUESTION 254
- (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 256
- (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 259
- (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 261
- (Exam Topic 2)
Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

A. Key performance indicators (KPIs)
B. Risk heat maps
C. Internal audit findings
D. Periodic penetration testing

Answer: A

NEW QUESTION 265
- (Exam Topic 2)
A risk practitioner is reviewing the status of an action plan to mitigate an emerging IT risk and finds the risk level has increased. The BEST course of action would be to:

A. implement the planned controls and accept the remaining risk.
B. suspend the current action plan in order to reassess the risk.
C. revise the action plan to include additional mitigating controls.
D. evaluate whether selected controls are still appropriate.

Answer: D

NEW QUESTION 268
- (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 272
- (Exam Topic 2)
Which of the following is the GREATEST risk associated with the use of data analytics?

A. Distributed data sources
B. Manual data extraction
C. Incorrect data selection
D. Excessive data volume

Answer: C

NEW QUESTION 273
- (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 275
- (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 276
- (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 278
- (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 282
- (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 285
- (Exam Topic 2)
A control owner has completed a year-long project To strengthen existing controls. It is MOST important for the risk practitioner to:

A. update the risk register to reflect the correct level of residual risk.
B. ensure risk monitoring for the project is initiated.
C. conduct and document a business impact analysis (BIA).
D. verify cost-benefit of the new controls betng implemented.

Answer: A

NEW QUESTION 286
- (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 287
- (Exam Topic 2)
During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

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

Answer: A

NEW QUESTION 290
- (Exam Topic 2)
Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

A. Obtain objective assessment of the control environment.
B. Ensure the risk profile is defined and communicated.
C. Validate the threat management process.
D. Obtain an objective view of process gaps and systemic errors.

Answer: A

NEW QUESTION 291
.....

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