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)
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 4
- (Exam Topic 1)
An organization is planning to engage a cloud-based service provider for some of its data-intensive business processes. Which of the following is MOST important to help define the IT risk associated with this outsourcing activity?

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

Answer: D

NEW QUESTION 5
- (Exam Topic 1)
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

Type	Scope	Completed By
External audit	Financial systems and processes	Third party
Internal audit	IT security risk management	Vendor
Vendor performance scorecard	Service level agreement compliance	Organization
Regulatory examination	Information security management program	Regulator

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

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
The acceptance of control costs that exceed risk exposure is MOST likely an example of:

A. low risk tolerance.

B. corporate culture misalignment.
C. corporate culture alignment.
D. high risk tolerance

Answer: B

NEW QUESTION 7
- (Exam Topic 1)
An organization has implemented a preventive control to lock user accounts after three unsuccessful login attempts. This practice has been proven to be unproductive, and a change in the control threshold value has been recommended. Who should authorize changing this threshold?

A. Risk owner
B. IT security manager
C. IT system owner
D. Control owner

Answer: D

NEW QUESTION 8
- (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 9
- (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 10
- (Exam Topic 1)
A risk practitioner is summarizing the results of a high-profile risk assessment sponsored by senior management. The BEST way to support risk-based decisions by senior management would be to:

A. map findings to objectives.
B. provide a quantified detailed analysts.
C. recommend risk tolerance thresholds.
D. quantify key risk indicators (KRIs).

Answer: A

NEW QUESTION 10
- (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 13
- (Exam Topic 1)
Which of the following is of GREATEST concern when uncontrolled changes are made to the control environment?

A. A decrease in control layering effectiveness
B. An increase in inherent risk
C. An increase in control vulnerabilities
D. An increase in the level of residual risk

Answer: D

NEW QUESTION 14

- (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 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 19
- (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)
A risk practitioner is organizing a training session lo communicate risk assessment methodologies to ensure a consistent risk view within the organization Which of the following i< the MOST important topic to cover in this training?

A. Applying risk appetite
B. Applying risk factors
C. Referencing risk event data
D. Understanding risk culture

Answer: D

NEW QUESTION 27
- (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 29
- (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 30
- (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 34
- (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 37
- (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 40
- (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 41
- (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 42
- (Exam Topic 1)
The PRIMARY objective for selecting risk response options is to:

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

Answer: A

NEW QUESTION 45
- (Exam Topic 1)
Which of the following is the PRIMARY factor in determining a recovery time objective (RTO)?

A. Cost of offsite backup premises
B. Cost of downtime due to a disaster
C. Cost of testing the business continuity plan
D. Response time of the emergency action plan

Answer: B

NEW QUESTION 50
- (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 53
- (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 54
- (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 58
- (Exam Topic 1)
A key risk indicator (KRI) is reported to senior management on a periodic basis as exceeding thresholds, but each time senior management has decided to take no action to reduce the risk. Which of the following is the MOST likely reason for senior management's response?

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

Answer: C

NEW QUESTION 62
- (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 67
- (Exam Topic 1)
Which of the following is the MAIN reason for documenting the performance of controls?

A. Obtaining management sign-off
B. Demonstrating effective risk mitigation
C. Justifying return on investment
D. Providing accurate risk reporting

Answer: D

NEW QUESTION 70
- (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 74
- (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 79
- (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 83
- (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 86
- (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 91
- (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 96
- (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 100
- (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 102
- (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 107
- (Exam Topic 1)
Which of the following is MOST helpful in identifying new risk exposures due to changes in the business environment?

A. Standard operating procedures
B. SWOT analysis
C. Industry benchmarking
D. Control gap analysis

Answer: B

NEW QUESTION 110
- (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 114
- (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 118
- (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 121
- (Exam Topic 1)
Which of the following would be- MOST helpful to understand the impact of a new technology system on an organization's current risk profile?

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

Answer: D

NEW QUESTION 125
- (Exam Topic 1)
Who should be accountable for ensuring effective cybersecurity controls are established?

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

Answer: B

NEW QUESTION 126

- (Exam Topic 1)
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 129
- (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 130
- (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 131
- (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 135
- (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 137
- (Exam Topic 1)
Which of the following would BEST help to ensure that identified risk is efficiently managed?

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

Answer: D

NEW QUESTION 138
- (Exam Topic 1)
Which of the following helps ensure compliance with a nonrepudiation policy requirement for electronic transactions?

A. Digital signatures
B. Encrypted passwords
C. One-time passwords
D. Digital certificates

Answer: A

NEW QUESTION 141
- (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 144
- (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 146
- (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 147
- (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 148
- (Exam Topic 1)
An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?

A. Perform a risk assessment
B. Disable user access.
C. Develop an access control policy.
D. Perform root cause analysis.

Answer: B

NEW QUESTION 152
- (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 153
- (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 158
- (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 160
- (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 162
- (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 164
- (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 166
- (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 169
- (Exam Topic 1)
An effective control environment is BEST indicated by controls that:

A. minimize senior management's risk tolerance.
B. manage risk within the organization's risk appetite.
C. reduce the thresholds of key risk indicators (KRIs).
D. are cost-effective to implement

Answer: B

NEW QUESTION 174
- (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 175
- (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 176
- (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 179
- (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 180
- (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 182
- (Exam Topic 1)
Improvements in the design and implementation of a control will MOST likely result in an update to:

A. inherent risk.
B. residual risk.
C. risk appetite
D. risk tolerance

Answer: B

NEW QUESTION 186
- (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 191

- (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 194
- (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 196
- (Exam Topic 2)
The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

A. assess gaps in IT risk management operations and strategic focus.
B. confirm that IT risk assessment results are expressed as business impact.
C. verify implemented controls to reduce the likelihood of threat materialization.
D. ensure IT risk management is focused on mitigating potential risk.

Answer: A

NEW QUESTION 197
- (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 198
- (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 200
- (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 201
- (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 203
- (Exam Topic 2)
Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

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

Answer: C

NEW QUESTION 206
- (Exam Topic 2)
Which of the following will BEST help an organization evaluate the control environment of several third-party vendors?

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

Answer: B

NEW QUESTION 209
- (Exam Topic 2)
Which of the following is the GREATEST concern when using a generic set of IT risk scenarios for risk analysis?

A. Quantitative analysis might not be possible.
B. Risk factors might not be relevant to the organization
C. Implementation costs might increase.
D. Inherent risk might not be considered.

Answer: B

NEW QUESTION 212
- (Exam Topic 2)
Which of the following should be the MOST important consideration when performing a vendor risk assessment?

A. Results of the last risk assessment of the vendor
B. Inherent risk of the business process supported by the vendor
C. Risk tolerance of the vendor
D. Length of time since the last risk assessment of the vendor

Answer: B

NEW QUESTION 213
- (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 216
- (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 217
- (Exam Topic 2)
The FIRST task when developing a business continuity plan should be to:

A. determine data backup and recovery availability at an alternate site.
B. identify critical business functions and resources.
C. define roles and responsibilities for implementation.
D. identify recovery time objectives (RTOs) for critical business applications.

Answer: B

NEW QUESTION 220
- (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 222
- (Exam Topic 2)
A bank wants to send a critical payment order via email to one of its offshore branches. Which of the following is the BEST way to ensure the message reaches the intended recipient without alteration?

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

Answer: C

NEW QUESTION 223
- (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 227
- (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 231
- (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 233
- (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 236
- (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 240
- (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 241
- (Exam Topic 2)
Deviation from a mitigation action plan's completion date should be determined by which of the following?

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

Answer: D

NEW QUESTION 242
- (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 243
- (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 248
- (Exam Topic 2)
Which of the following should be considered when selecting a risk response?

A. Risk scenarios analysis
B. Risk response costs
C. Risk factor awareness
D. Risk factor identification

Answer: B

NEW QUESTION 250
- (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 254
- (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 255
- (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 260
- (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 264
- (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 269
- (Exam Topic 2)
Management has required information security awareness training to reduce the risk associated with credential compromise. What is the BEST way to assess the effectiveness of the training?

A. Conduct social engineering testing.
B. Audit security awareness training materials.
C. Administer an end-of-training quiz.
D. Perform a vulnerability assessment.

Answer: A

NEW QUESTION 274
- (Exam Topic 2)
IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

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

Answer: D

NEW QUESTION 279
- (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 283

- (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 286
- (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 290
- (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 291
- (Exam Topic 2)
Which of the following is MOST important to understand when developing key risk indicators (KRIs)?

A. KRI thresholds
B. Integrity of the source data
C. Control environment
D. Stakeholder requirements

Answer: A

NEW QUESTION 295
- (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 298
- (Exam Topic 2)
A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (PII). Which of the following will MOST likely outcome for an organization affected by the new law?

A. Increase in compliance breaches
B. Increase in loss event impact
C. Increase in residual risk
D. Increase in customer complaints

Answer: B

NEW QUESTION 301
- (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 302
- (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 306
- (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 311
- (Exam Topic 2)
What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium	Low	Low
Tango	Medium	Low	Medium
Uniform	High	High	High
Victor	High	Medium	Medium

A. Relative positions on the risk map
B. Risk treatment options
C. Capability of enterprise to implement
D. The multiple risk factors addressed by a chosen response

Answer: A

NEW QUESTION 315
- (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 316
- (Exam Topic 2)
Which of the following provides the MOST important information to facilitate a risk response decision?

A. Audit findings
B. Risk appetite
C. Key risk indicators
D. Industry best practices

Answer: B

NEW QUESTION 321
- (Exam Topic 2)
An organization has decided to outsource a web application, and customer data will be stored in the vendor's public cloud. To protect customer data, it is MOST important to ensure which of the following?

A. The organization's incident response procedures have been updated.
B. The vendor stores the data in the same jurisdiction.
C. Administrative access is only held by the vendor.
D. The vendor's responsibilities are defined in the contract.

Answer: D

NEW QUESTION 326
- (Exam Topic 2)
When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

A. business process objectives have been met.
B. control adheres to regulatory standards.
C. residual risk objectives have been achieved.
D. control process is designed effectively.

Answer: C

NEW QUESTION 329
- (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 330
- (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 331
- (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 336
- (Exam Topic 2)
A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

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

Answer: B

NEW QUESTION 338
- (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 341
- (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 343
- (Exam Topic 2)
Which of the following is MOST important for an organization that wants to reduce IT operational risk?

A. Increasing senior management's understanding of IT operations
B. Increasing the frequency of data backups
C. Minimizing complexity of IT infrastructure
D. Decentralizing IT infrastructure

Answer: D

NEW QUESTION 348
- (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 353
- (Exam Topic 2)
When reporting on the performance of an organization's control environment including which of the following would BEST inform stakeholders risk decision-making?

A. The audit plan for the upcoming period
B. Spend to date on mitigating control implementation
C. A report of deficiencies noted during controls testing
D. A status report of control deployment

Answer: C

NEW QUESTION 357
- (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 361
- (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 364
- (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 369
......

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