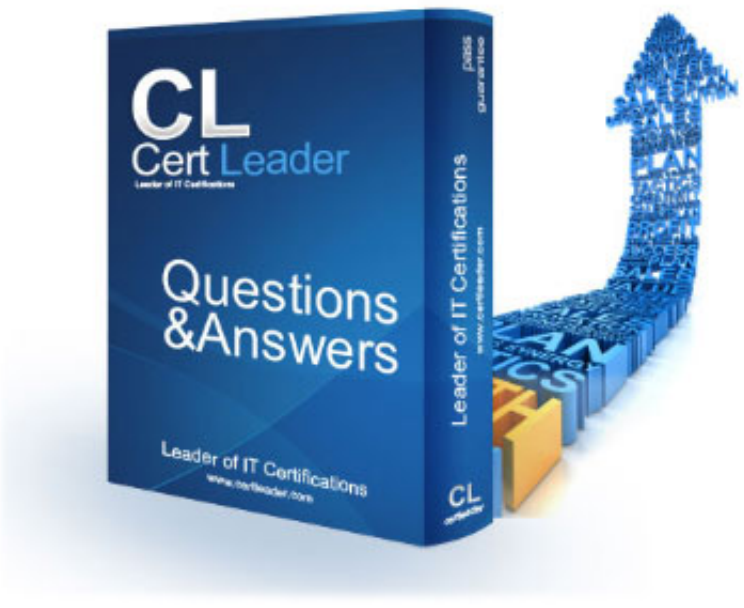
CRISC Dumps

Certified in Risk and Information Systems Control

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



NEW QUESTION 1
- (Exam Topic 4)
What is the MAIN benefit of using a top-down approach to develop risk scenarios?

A. It describes risk events specific to technology used by the enterprise.
B. It establishes the relationship between risk events and organizational objectives.
C. It uses hypothetical and generic risk events specific to the enterprise.
D. It helps management and the risk practitioner to refine risk scenarios.

Answer: C

NEW QUESTION 2
- (Exam Topic 4)
Which of the following would provide the MOST useful input when evaluating the appropriateness of risk responses?

A. Incident reports
B. Cost-benefit analysis
C. Risk tolerance
D. Control objectives

Answer: B

NEW QUESTION 3
- (Exam Topic 4)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

A. Management approval
B. Annual review
C. Relevance
D. Automation

Answer: A

NEW QUESTION 4
- (Exam Topic 4)
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, program for all employees of the organization?

A. Recovery time objectives (RTOs)
B. Segregation of duties
C. Communication plan
D. Critical asset inventory

Answer: C

NEW QUESTION 5
- (Exam Topic 4)
Which of the following would provide the MOST reliable evidence of the effectiveness of security controls implemented for a web application?

A. Penetration testing
B. IT general controls audit
C. Vulnerability assessment
D. Fault tree analysis

Answer: A

NEW QUESTION 6
- (Exam Topic 4)
A poster has been displayed in a data center that reads. "Anyone caught taking photographs in the data center may be subject to disciplinary action." Which of the following control types has been implemented?

A. Corrective
B. Detective
C. Deterrent
D. Preventative

Answer: A

NEW QUESTION 7
- (Exam Topic 4)
When a risk practitioner is determining a system's criticality. it is MOST helpful to review the associated:

A. process flow.
B. business impact analysis (BIA).
C. service level agreement (SLA).
D. system architecture.

Answer: B

NEW QUESTION 8
- (Exam Topic 4)
Which of the following key performance indicators (KPis) would BEST measure me risk of a service outage when using a Software as a Service (SaaS) vendors

A. Frequency of business continuity plan (BCP) lasting
B. Frequency and number of new software releases
C. Frequency and duration of unplanned downtime
D. Number of IT support staff available after business hours

Answer: C

NEW QUESTION 9
- (Exam Topic 4)
An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

A. Threat
B. Risk
C. Vulnerability
D. Policy violation

Answer: B

NEW QUESTION 10
- (Exam Topic 4)
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

A. Several risk action plans have missed target completion dates.
B. Senior management has accepted more risk than usual.
C. Risk associated with many assets is only expressed in qualitative terms.
D. Many risk scenarios are owned by the same senior manager.

Answer: A

NEW QUESTION 10
- (Exam Topic 4)
Which of the following would be of MOST concern to a risk practitioner reviewing risk action plans for documented IT risk scenarios?

A. Individuals outside IT are managing action plans for the risk scenarios.
B. Target dates for completion are missing from some action plans.
C. Senior management approved multiple changes to several action plans.
D. Many action plans were discontinued after senior management accepted the risk.

Answer: B

NEW QUESTION 15
- (Exam Topic 4)
Which of the following roles should be assigned accountability for monitoring risk levels?

A. Risk practitioner
B. Business manager
C. Risk owner
D. Control owner

Answer: C

NEW QUESTION 20
- (Exam Topic 4)
An organization's control environment is MOST effective when:

A. controls perform as intended.
B. controls operate efficiently.
C. controls are implemented consistent
D. control designs are reviewed periodically

Answer: A

NEW QUESTION 22
- (Exam Topic 4)
Which component of a software inventory BEST enables the identification and mitigation of known vulnerabilities?

A. Software version

B. Assigned software manager
C. Software support contract expiration
D. Software licensing information

Answer: A

NEW QUESTION 24
- (Exam Topic 4)
A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

A. risk score
B. risk impact
C. risk response
D. risk likelihood.

Answer: B

NEW QUESTION 27
- (Exam Topic 4)
Which of the following would provide the BEST evidence of an effective internal control environment/?

A. Risk assessment results
B. Adherence to governing policies
C. Regular stakeholder briefings
D. Independent audit results

Answer: D

NEW QUESTION 31
- (Exam Topic 4)
An organization has decided to commit to a business activity with the knowledge that the risk exposure is higher than the risk appetite. Which of the following is the risk practitioner's MOST important action related to this decision?

A. Recommend risk remediation
B. Change the level of risk appetite
C. Document formal acceptance of the risk
D. Reject the business initiative

Answer: C

NEW QUESTION 35
- (Exam Topic 4)
Which of the following is the PRIMARY reason for a risk practitioner to review an organization's IT asset inventory?

A. To plan for the replacement of assets at the end of their life cycles
B. To assess requirements for reducing duplicate assets
C. To understand vulnerabilities associated with the use of the assets
D. To calculate mean time between failures (MTBF) for the assets

Answer: C

NEW QUESTION 36
- (Exam Topic 4)
Which of the following practices would be MOST effective in protecting personality identifiable information (Ptl) from unauthorized access m a cloud environment?

A. Apply data classification policy
B. Utilize encryption with logical access controls
C. Require logical separation of company data
D. Obtain the right to audit

Answer: B

NEW QUESTION 39
- (Exam Topic 4)
Which of the following would be a risk practitioner's GREATEST concern with the use of a vulnerability scanning tool?

A. Increased time to remediate vulnerabilities
B. Inaccurate reporting of results
C. Increased number of vulnerabilities
D. Network performance degradation

Answer: B

NEW QUESTION 40

- (Exam Topic 4)
Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

A. Gap analysis
B. Threat assessment
C. Resource skills matrix
D. Data quality assurance plan

Answer: A

NEW QUESTION 44
- (Exam Topic 4)
An organization has asked an IT risk practitioner to conduct an operational risk assessment on an initiative to outsource the organization's customer service operations overseas. Which of the following would MOST significantly impact management's decision?

A. Time zone difference of the outsourcing location
B. Ongoing financial viability of the outsourcing company
C. Cross-border information transfer restrictions in the outsourcing country
D. Historical network latency between the organization and outsourcing location

Answer: C

NEW QUESTION 47
- (Exam Topic 4)
Which of the following is MOST likely to introduce risk for financial institutions that use blockchain?

A. Cost of implementation
B. Implementation of unproven applications
C. Disruption to business processes
D. Increase in attack surface area

Answer: B

NEW QUESTION 52
- (Exam Topic 4)
Which of the following is the MOST important consideration when developing risk strategies?

A. Organization's industry sector
B. Long-term organizational goals
C. Concerns of the business process owners
D. History of risk events

Answer: B

NEW QUESTION 57
- (Exam Topic 4)
Which of The following BEST represents the desired risk posture for an organization?

A. Inherent risk is lower than risk tolerance.
B. Operational risk is higher than risk tolerance.
C. Accepted risk is higher than risk tolerance.
D. Residual risk is lower than risk tolerance.

Answer: D

NEW QUESTION 60
- (Exam Topic 4)
Which of the following is the BEST way to validate whether controls to reduce user device vulnerabilities have been implemented according to management's action plan?

A. Survey device owners.
B. Rescan the user environment.
C. Require annual end user policy acceptance.
D. Review awareness training assessment results

Answer: B

NEW QUESTION 61
- (Exam Topic 4)
Which of the following is the PRIMARY purpose of creating and documenting control procedures?

A. To facilitate ongoing audit and control testing
B. To help manage risk to acceptable tolerance levels
C. To establish and maintain a control inventory
D. To increase the likelihood of effective control operation

Answer: D

NEW QUESTION 65
- (Exam Topic 3)
Which of the following BEST measures the impact of business interruptions caused by an IT service outage?

A. Sustained financial loss
B. Cost of remediation efforts
C. Duration of service outage
D. Average time to recovery

Answer: A

NEW QUESTION 68
- (Exam Topic 4)
An organization has allowed several employees to retire early in order to avoid layoffs Many of these employees have been subject matter experts for critical assets Which type of risk is MOST likely to materialize?

A. Confidentiality breach
B. Institutional knowledge loss
C. Intellectual property loss
D. Unauthorized access

Answer: B

NEW QUESTION 70
- (Exam Topic 4)
A penetration test reveals several vulnerabilities in a web-facing application. Which of the following should be the FIRST step in selecting a risk response?

A. Correct the vulnerabilities to mitigate potential risk exposure.
B. Develop a risk response action plan with key stakeholders.
C. Assess the level of risk associated with the vulnerabilities.
D. Communicate the vulnerabilities to the risk owner.

Answer: C

NEW QUESTION 74
- (Exam Topic 4)
Which of the following is MOST important to consider before determining a response to a vulnerability?

A. The likelihood and impact of threat events
B. The cost to implement the risk response
C. Lack of data to measure threat events
D. Monetary value of the asset

Answer: C

NEW QUESTION 76
- (Exam Topic 3)
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 77
- (Exam Topic 3)
Which of the following is the MOST effective control to maintain the integrity of system configuration files?

A. Recording changes to configuration files
B. Implementing automated vulnerability scanning
C. Restricting access to configuration documentation
D. Monitoring against the configuration standard

Answer: D

NEW QUESTION 82
- (Exam Topic 3)
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: B

NEW QUESTION 83
- (Exam Topic 3)
The MAIN reason for creating and maintaining a risk register is to:

A. assess effectiveness of different projects.
B. define the risk assessment methodology.
C. ensure assets have low residual risk.
D. account for identified key risk factors.

Answer: D

NEW QUESTION 87
- (Exam Topic 3)
A financial institution has identified high risk of fraud in several business applications. Which of the following controls will BEST help reduce the risk of fraudulent internal transactions?

A. Periodic user privileges review
B. Log monitoring
C. Periodic internal audits
D. Segregation of duties

Answer: A

NEW QUESTION 91
- (Exam Topic 3)
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: D

NEW QUESTION 96
- (Exam Topic 3)
Which of the following is MOST helpful in preventing risk events from materializing?

A. Prioritizing and tracking issues
B. Establishing key risk indicators (KRIs)
C. Reviewing and analyzing security incidents
D. Maintaining the risk register

Answer: A

NEW QUESTION 99
- (Exam Topic 3)
The PRIMARY benefit associated with key risk indicators (KRIs) is that they:

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

Answer: D

NEW QUESTION 101
- (Exam Topic 3)
Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

A. Vulnerability scanning
B. Systems log correlation analysis
C. Penetration testing
D. Monitoring of intrusion detection system (IDS) alerts

Answer: C

NEW QUESTION 103
- (Exam Topic 3)
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 107
- (Exam Topic 3)
Which of the following should be the FIRST consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected?

A. Informed consent
B. Cross border controls
C. Business impact analysis (BIA)
D. Data breach protection

Answer: A

NEW QUESTION 108
- (Exam Topic 3)
A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

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

Answer: D

NEW QUESTION 110
- (Exam Topic 3)
An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

A. Potential increase in regulatory scrutiny
B. Potential system downtime
C. Potential theft of personal information
D. Potential legal risk

Answer: C

NEW QUESTION 112
- (Exam Topic 3)
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 113
- (Exam Topic 3)
Which of the following is the MOST important topic to cover in a risk awareness training program for all staff?

A. Internal and external information security incidents
B. The risk department's roles and responsibilities
C. Policy compliance requirements and exceptions process
D. The organization's information security risk profile

Answer: C

NEW QUESTION 114
- (Exam Topic 3)
Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

A. Perform a return on investment analysis.
B. Review the risk register and risk scenarios.
C. Calculate annualized loss expectancy of risk scenarios.
D. Raise the maturity of organizational risk management.

Answer: D

NEW QUESTION 117

- (Exam Topic 3)
A service provider is managing a client's servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider's MOST appropriate action would be to:

A. develop a risk remediation plan overriding the client's decision
B. make a note for this item in the next audit explaining the situation
C. insist that the remediation occur for the benefit of other customers
D. ask the client to document the formal risk acceptance for the provider

Answer: D

NEW QUESTION 119
- (Exam Topic 3)
An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?

A. Risk manager
B. Data owner
C. End user
D. IT department

Answer: D

NEW QUESTION 121
- (Exam Topic 3)
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 125
- (Exam Topic 3)
Which of the following should be the GREATEST concern for an organization that uses open source software applications?

A. Lack of organizational policy regarding open source software
B. Lack of reliability associated with the use of open source software
C. Lack of monitoring over installation of open source software in the organization
D. Lack of professional support for open source software

Answer: A

NEW QUESTION 127
- (Exam Topic 3)
Which of the following is the PRIMARY benefit of using an entry in the risk register to track the aggregate risk associated with server failure?

A. It provides a cost-benefit analysis on control options available for implementation.
B. It provides a view on where controls should be applied to maximize the uptime of servers.
C. It provides historical information about the impact of individual servers malfunctioning.
D. It provides a comprehensive view of the impact should the servers simultaneously fail.

Answer: D

NEW QUESTION 130
- (Exam Topic 3)
Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

A. Automated access revocation
B. Daily transaction reconciliation
C. Rule-based data analytics
D. Role-based user access model

Answer: B

NEW QUESTION 134
- (Exam Topic 3)
Risk acceptance of an exception to a security control would MOST likely be justified when:

A. automation cannot be applied to the control
B. business benefits exceed the loss exposure.
C. the end-user license agreement has expired.
D. the control is difficult to enforce in practice.

Answer: B

NEW QUESTION 139
- (Exam Topic 3)
Which of the following is the PRIMARY risk management responsibility of the second line of defense?

A. Monitoring risk responses
B. Applying risk treatments
C. Providing assurance of control effectiveness
D. Implementing internal controls

Answer: A

NEW QUESTION 140
- (Exam Topic 3)
Which of the following is MOST important when developing key risk indicators (KRIs)?

A. Alignment with regulatory requirements
B. Availability of qualitative data
C. Properly set thresholds
D. Alignment with industry benchmarks

Answer: C

NEW QUESTION 142
- (Exam Topic 3)
Which of the following BEST indicates the condition of a risk management program?

A. Number of risk register entries
B. Number of controls
C. Level of financial support
D. Amount of residual risk

Answer: D

NEW QUESTION 145
- (Exam Topic 3)
Which of the following is the BEST indication of a mature organizational risk culture?

A. Corporate risk appetite is communicated to staff members.
B. Risk owners understand and accept accountability for risk.
C. Risk policy has been published and acknowledged by employees.
D. Management encourages the reporting of policy breaches.

Answer: B

NEW QUESTION 150
- (Exam Topic 3)
Determining if organizational risk is tolerable requires:

A. mapping residual risk with cost of controls
B. comparing against regulatory requirements
C. comparing industry risk appetite with the organization's.
D. understanding the organization's risk appetite.

Answer: D

NEW QUESTION 152
- (Exam Topic 3)
Which of the following should be determined FIRST when a new security vulnerability is made public?

A. Whether the affected technology is used within the organization
B. Whether the affected technology is Internet-facing
C. What mitigating controls are currently in place
D. How pervasive the vulnerability is within the organization

Answer: A

NEW QUESTION 155
- (Exam Topic 3)
Which of the following is the BEST evidence that a user account has been properly authorized?

A. An email from the user accepting the account
B. Notification from human resources that the account is active
C. User privileges matching the request form
D. Formal approval of the account by the user's manager

Answer:

C

NEW QUESTION 156
- (Exam Topic 3)
The MOST important objective of information security controls is to:

A. Identify threats and vulnerability
B. Ensure alignment with industry standards
C. Provide measurable risk reduction
D. Enforce strong security solutions

Answer: C

NEW QUESTION 158
- (Exam Topic 3)
Which of the following should be the risk practitioner's FIRST course of action when an organization plans to adopt a cloud computing strategy?

A. Request a budget for implementation
B. Conduct a threat analysis.
C. Create a cloud computing policy.
D. Perform a controls assessment.

Answer: B

NEW QUESTION 162
- (Exam Topic 3)
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 163
- (Exam Topic 3)
Who should have the authority to approve an exception to a control?

A. information security manager
B. Control owner
C. Risk owner
D. Risk manager

Answer: C

NEW QUESTION 166
- (Exam Topic 3)
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 171
- (Exam Topic 3)
Which of the following is the PRIMARY role of a data custodian in the risk management process?

A. Performing periodic data reviews according to policy
B. Reporting and escalating data breaches to senior management
C. Being accountable for control design
D. Ensuring data is protected according to the classification

Answer: D

NEW QUESTION 172
- (Exam Topic 3)
When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs?

A. Risk management
B. Change management
C. Problem management

D. Quality management

Answer: B

NEW QUESTION 175
- (Exam Topic 3)
Which of the following provides the MOST useful information when determining if a specific control should be implemented?

A. Business impact analysis (BIA)
B. Cost-benefit analysis
C. Attribute analysis
D. Root cause analysis

Answer: B

NEW QUESTION 176
- (Exam Topic 3)
Which of the following is the PRIMARY reason to use key control indicators (KCIs) to evaluate control operating effectiveness?

A. To measure business exposure to risk
B. To identify control vulnerabilities
C. To monitor the achievement of set objectives
D. To raise awareness of operational issues

Answer: C

NEW QUESTION 180
- (Exam Topic 3)
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 181
- (Exam Topic 3)
Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:

A. is in charge of information security.
B. is responsible for enterprise risk management (ERM)
C. can implement remediation action plans.
D. is accountable for loss if the risk materializes.

Answer: D

NEW QUESTION 186
- (Exam Topic 3)
A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

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

Answer: D

NEW QUESTION 188
- (Exam Topic 3)
A risk practitioner is preparing a report to communicate changes in the risk and control environment. The BEST way to engage stakeholder attention is to:

A. include detailed deviations from industry benchmarks,
B. include a summary linking information to stakeholder needs,
C. include a roadmap to achieve operational excellence,
D. publish the report on-demand for stakeholders.

Answer: B

NEW QUESTION 193
- (Exam Topic 3)
Which of the following provides the MOST useful information to determine risk exposure following control implementations?

A. Strategic plan and risk management integration
B. Risk escalation and process for communication
C. Risk limits, thresholds, and indicators
D. Policies, standards, and procedures

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
Which of the following would BEST assist in reconstructing the sequence of events following a security incident across multiple IT systems in the organization's network?

A. Network monitoring infrastructure
B. Centralized vulnerability management
C. Incident management process
D. Centralized log management

Answer: D

NEW QUESTION 199
- (Exam Topic 3)
Which of the following is the BEST reason to use qualitative measures to express residual risk levels related to emerging threats?

A. Qualitative measures require less ongoing monitoring.
B. Qualitative measures are better aligned to regulatory requirements.
C. Qualitative measures are better able to incorporate expert judgment.
D. Qualitative measures are easier to update.

Answer: C

NEW QUESTION 203
- (Exam Topic 3)
An organization is conducting a review of emerging risk. Which of the following is the BEST input for this exercise?

A. Audit reports
B. Industry benchmarks
C. Financial forecasts
D. Annual threat reports

Answer: B

NEW QUESTION 208
- (Exam Topic 3)
Which of the following practices MOST effectively safeguards the processing of personal data?

A. Personal data attributed to a specific data subject is tokenized.
B. Data protection impact assessments are performed on a regular basis.
C. Personal data certifications are performed to prevent excessive data collection.
D. Data retention guidelines are documented, established, and enforced.

Answer: B

NEW QUESTION 211
- (Exam Topic 3)
Which of the following will be MOST effective in uniquely identifying the originator of electronic transactions?

A. Digital signature
B. Edit checks
C. Encryption
D. Multifactor authentication

Answer: A

NEW QUESTION 216
- (Exam Topic 3)
Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

A. Financial risk is given a higher priority.
B. Risk with strategic impact is included.
C. Security strategy is given a higher priority.
D. Risk identified by industry benchmarking is included.

Answer: B

NEW QUESTION 217

- (Exam Topic 3)
A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?

A. Third-party software is used for data analytics.
B. Data usage exceeds individual consent.
C. Revenue generated is not disclosed to customers.
D. Use of a data analytics system is not disclosed to customers.

Answer: B

NEW QUESTION 219
- (Exam Topic 3)
An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?

A. Migrate all data to another compliant service provider.
B. Analyze the impact of the provider's control weaknesses to the business.
C. Conduct a follow-up audit to verify the provider's control weaknesses.
D. Review the contract to determine if penalties should be levied against the provider.

Answer: B

NEW QUESTION 222
- (Exam Topic 3)
An organization outsources the processing of us payroll data A risk practitioner identifies a control weakness at the third party trial exposes the payroll data. Who should own this risk?

A. The third party's IT operations manager
B. The organization's process owner
C. The third party's chief risk officer (CRO)
D. The organization's risk practitioner

Answer: B

NEW QUESTION 226
- (Exam Topic 3)
Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?

A. Ongoing availability of data
B. Ability to aggregate data
C. Ability to predict trends
D. Availability of automated reporting systems

Answer: D

NEW QUESTION 227
- (Exam Topic 3)
When evaluating enterprise IT risk management it is MOST important to:

A. create new control processes to reduce identified IT risk scenarios
B. confirm the organization’s risk appetite and tolerance
C. report identified IT risk scenarios to senior management
D. review alignment with the organization's investment plan

Answer: B

NEW QUESTION 228
- (Exam Topic 3)
Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures?

A. Mean time to recover (MTTR)
B. IT system criticality classification
C. Incident management service level agreement (SLA)
D. Recovery time objective (RTO)

Answer: D

NEW QUESTION 231
- (Exam Topic 3)
Which of the following data would be used when performing a business impact analysis (BIA)?

A. Cost-benefit analysis of running the current business
B. Cost of regulatory compliance
C. Projected impact of current business on future business
D. Expected costs for recovering the business

Answer: D

NEW QUESTION 233
- (Exam Topic 3)
Which of the following is the MOST important consideration when sharing risk management updates with executive management?

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

Answer: D

NEW QUESTION 236
- (Exam Topic 3)
The PRIMARY advantage of involving end users in continuity planning is that they:

A. have a better understanding of specific business needs
B. can balance the overall technical and business concerns
C. can see the overall impact to the business
D. are more objective than information security management.

Answer: B

NEW QUESTION 240
- (Exam Topic 3)
What is the PRIMARY benefit of risk monitoring?

A. It reduces the number of audit findings.
B. It provides statistical evidence of control efficiency.
C. It facilitates risk-aware decision making.
D. It facilitates communication of threat levels.

Answer: C

NEW QUESTION 241
- (Exam Topic 3)
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 242
- (Exam Topic 3)
Which of the following is MOST important to the successful development of IT risk scenarios?

A. Cost-benefit analysis
B. Internal and external audit reports
C. Threat and vulnerability analysis
D. Control effectiveness assessment

Answer: C

NEW QUESTION 245
- (Exam Topic 3)
Which of the following would be MOST useful to senior management when determining an appropriate risk response?

A. A comparison of current risk levels with established tolerance
B. A comparison of cost variance with defined response strategies
C. A comparison of current risk levels with estimated inherent risk levels
D. A comparison of accepted risk scenarios associated with regulatory compliance

Answer: A

NEW QUESTION 248
- (Exam Topic 3)
What should be the PRIMARY driver for periodically reviewing and adjusting key risk indicators (KRIs)?

A. Risk impact
B. Risk likelihood

C. Risk appropriate
D. Control self-assessments (CSAs)

Answer: B

NEW QUESTION 249
- (Exam Topic 3)
Analyzing trends in key control indicators (KCIs) BEST enables a risk practitioner to proactively identify impacts on an organization's:

A. risk classification methods
B. risk-based capital allocation
C. risk portfolio
D. risk culture

Answer: C

NEW QUESTION 254
- (Exam Topic 3)
Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

A. Conducting a business impact analysis (BIA)
B. Identifying the recovery response team
C. Procuring a recovery site
D. Assigning sensitivity levels to data

Answer: A

NEW QUESTION 259
- (Exam Topic 3)
Which of the following should be the PRIMARY focus of an IT risk awareness program?

A. Ensure compliance with the organization's internal policies
B. Cultivate long-term behavioral change.
C. Communicate IT risk policy to the participants.
D. Demonstrate regulatory compliance.

Answer: B

NEW QUESTION 260
- (Exam Topic 3)
Which of the following approaches BEST identifies information systems control deficiencies?

A. Countermeasures analysis
B. Best practice assessment
C. Gap analysis
D. Risk assessment

Answer: C

NEW QUESTION 263
- (Exam Topic 3)
Which of The following is the MOST comprehensive input to the risk assessment process specific to the effects of system downtime?

A. Business continuity plan (BCP) testing results
B. Recovery lime objective (RTO)
C. Business impact analysis (BIA)
D. results Recovery point objective (RPO)

Answer: C

NEW QUESTION 264
- (Exam Topic 3)
Which of the following controls BEST enables an organization to ensure a complete and accurate IT asset inventory?

A. Prohibiting the use of personal devices for business
B. Performing network scanning for unknown devices
C. Requesting an asset list from business owners
D. Documenting asset configuration baselines

Answer: B

NEW QUESTION 265
- (Exam Topic 3)
Which of the following methods is an example of risk mitigation?

A. Not providing capability for employees to work remotely
B. Outsourcing the IT activities and infrastructure
C. Enforcing change and configuration management processes
D. Taking out insurance coverage for IT-related incidents

Answer: C

NEW QUESTION 270
- (Exam Topic 3)
Which of the following is the BEST way to quantify the likelihood of risk materialization?

A. Balanced scorecard
B. Threat and vulnerability assessment
C. Compliance assessments
D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 272
- (Exam Topic 3)
An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:

A. reduce the likelihood of future events
B. restore availability
C. reduce the impact of future events
D. address the root cause

Answer: D

NEW QUESTION 273
- (Exam Topic 3)
Which of the following is the BEST source for identifying key control indicators (KCIs)?

A. Privileged user activity monitoring controls
B. Controls mapped to organizational risk scenarios
C. Recent audit findings of control weaknesses
D. A list of critical security processes

Answer: B

NEW QUESTION 277
- (Exam Topic 3)
Who is BEST suited to determine whether a new control properly mitigates data loss risk within a system?

A. Data owner
B. Control owner
C. Risk owner
D. System owner

Answer: B

NEW QUESTION 280
- (Exam Topic 3)
Days before the realization of an acquisition, a data breach is discovered at the company to be acquired. For the accruing organization, this situation represents which of the following?

A. Threat event
B. Inherent risk
C. Risk event
D. Security incident

Answer: B

NEW QUESTION 284
- (Exam Topic 3)
An organization learns of a new ransomware attack affecting organizations worldwide. Which of the following should be done FIRST to reduce the likelihood of infection from the attack?

A. Identify systems that are vulnerable to being exploited by the attack.
B. Confirm with the antivirus solution vendor whether the next update will detect the attack.
C. Verify the data backup process and confirm which backups are the most recent ones available.
D. Obtain approval for funding to purchase a cyber insurance plan.

Answer: A

NEW QUESTION 288
- (Exam Topic 3)
To help identify high-risk situations, an organization should:

A. continuously monitor the environment.
B. develop key performance indicators (KPIs).
C. maintain a risk matrix.
D. maintain a risk register.

Answer: A

NEW QUESTION 289
- (Exam Topic 3)
Which of We following is the MOST effective control to address the risk associated with compromising data privacy within the cloud?

A. Establish baseline security configurations with the cloud service provider.
B. Require the cloud prowler 10 disclose past data privacy breaches.
C. Ensure the cloud service provider performs an annual risk assessment.
D. Specify cloud service provider liability for data privacy breaches in the contract

Answer: D

NEW QUESTION 292
- (Exam Topic 3)
A highly regulated organization acquired a medical technology startup company that processes sensitive personal information with weak data protection controls. Which of the following is the BEST way for the
acquiring company to reduce its risk while still enabling the flexibility needed by the startup company?

A. Identify previous data breaches using the startup company’s audit reports.
B. Have the data privacy officer review the startup company’s data protection policies.
C. Classify and protect the data according to the parent company's internal standards.
D. Implement a firewall and isolate the environment from the parent company's network.

Answer: A

NEW QUESTION 297
- (Exam Topic 3)
Print jobs containing confidential information are sent to a shared network printer located in a secure room. Which of the following is the BEST control to prevent the inappropriate disclosure of confidential information?

A. Requiring a printer access code for each user
B. Using physical controls to access the printer room
C. Using video surveillance in the printer room
D. Ensuring printer parameters are properly configured

Answer: A

NEW QUESTION 298
- (Exam Topic 3)
Which of The following should be the FIRST step when a company is made aware of new regulatory requirements impacting IT?

A. Perform a gap analysis.
B. Prioritize impact to the business units.
C. Perform a risk assessment.
D. Review the risk tolerance and appetite.

Answer: C

NEW QUESTION 301
- (Exam Topic 3)
All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

A. select a provider to standardize the disaster recovery plans.
B. outsource disaster recovery to an external provider.
C. centralize the risk response function at the enterprise level.
D. evaluate opportunities to combine disaster recovery plans.

Answer: D

NEW QUESTION 305
- (Exam Topic 4)
The objective of aligning mitigating controls to risk appetite is to ensure that:

A. exposures are reduced to the fullest extent
B. exposures are reduced only for critical business systems
C. insurance costs are minimized

D. the cost of controls does not exceed the expected loss.

Answer: D

NEW QUESTION 309
- (Exam Topic 4)
Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

A. Board of directors
B. Vendors
C. Regulators
D. Legal team

Answer: A

NEW QUESTION 311
- (Exam Topic 4)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

A. Prioritize risk response options
B. Reduce likelihood.
C. Address more than one risk response
D. Reduce impact

Answer: C

NEW QUESTION 315
- (Exam Topic 4)
Which of the following is MOST helpful to understand the consequences of an IT risk event?

A. Fault tree analysis
B. Historical trend analysis
C. Root cause analysis
D. Business impact analysis (BIA)

Answer: B

NEW QUESTION 317
- (Exam Topic 4)
An organization has an approved bring your own device (BYOD) policy. Which of the following would BEST mitigate the security risk associated with the inappropriate use of enterprise applications on the devices?

A. Periodically review application on BYOD devices
B. Include BYOD in organizational awareness programs
C. Implement BYOD mobile device management (MDM) controls.
D. Enable a remote wee capability for BYOD devices

Answer: C

NEW QUESTION 319
- (Exam Topic 4)
Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?

A. Data classification policy
B. Emerging technology trends
C. The IT strategic plan
D. The risk register

Answer: C

NEW QUESTION 320
- (Exam Topic 4)
Which of the following BEST enables a risk practitioner to understand management's approach to organizational risk?

A. Organizational structure and job descriptions
B. Risk appetite and risk tolerance
C. Industry best practices for risk management
D. Prior year's risk assessment results

Answer: B

NEW QUESTION 322
- (Exam Topic 4)
An organization has completed a risk assessment of one of its service providers. Who should be accountable for ensuring that risk responses are implemented?

A. IT risk practitioner
B. Third -partf3ecurity team
C. The relationship owner
D. Legal representation of the business

Answer: C

NEW QUESTION 323
- (Exam Topic 4)
Which of the following provides the MOST useful information to assess the magnitude of identified deficiencies in the IT control environment?

A. Peer benchmarks
B. Internal audit reports
C. Business impact analysis (BIA) results
D. Threat analysis results

Answer: D

NEW QUESTION 328
- (Exam Topic 4)
Which of the following BEST enables senior management lo compare the ratings of risk scenarios?

A. Key risk indicators (KRIs)
B. Key performance indicators (KPIs)
C. Control self-assessment (CSA)
D. Risk heat map

Answer: D

NEW QUESTION 333
- (Exam Topic 4)
Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board"

A. A summary of risk response plans with validation results
B. A report with control environment assessment results
C. A dashboard summarizing key risk indicators (KRIs)
D. A summary of IT risk scenarios with business cases

Answer: C

NEW QUESTION 335
- (Exam Topic 4)
An organization is analyzing the risk of shadow IT usage. Which of the following is the MOST important input into the assessment?

A. Business benefits of shadow IT
B. Application-related expresses
C. Classification of the data
D. Volume of data

Answer: A

NEW QUESTION 337
- (Exam Topic 4)
Which of the following would BEST facilitate the implementation of data classification requirements?

A. Implementing a data toss prevention (DLP) solution
B. Assigning a data owner
C. Scheduling periodic audits
D. Implementing technical controls over the assets

Answer: B

NEW QUESTION 341
- (Exam Topic 4)
Which of the following has the GREATEST influence on an organization's risk appetite?

A. Threats and vulnerabilities
B. Internal and external risk factors
C. Business objectives and strategies
D. Management culture and behavior

Answer: D

NEW QUESTION 346
- (Exam Topic 4)

Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

A. KRIs assist in the preparation of the organization's risk profile.
B. KRIs signal that a change in the control environment has occurred.
C. KRIs provide a basis to set the risk appetite for an organization
D. KRIs provide an early warning that a risk threshold is about to be reached.

Answer: D

NEW QUESTION 351
- (Exam Topic 4)
Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

A. Ensuring processes are documented to enable effective control execution
B. Ensuring regular risk messaging is Included in business communications from leadership
C. Ensuring schedules and deadlines for control-related deliverables are strictly monitored
D. Ensuring performance metrics balance business goals with risk appetiie

Answer: B

NEW QUESTION 354
- (Exam Topic 4)
When of the following standard operating procedure (SOP) statements BEST illustrates appropriate risk register maintenance?

A. Remove risk that has been mitigated by third-party transfer
B. Remove risk that management has decided to accept
C. Remove risk only following a significant change in the risk environment
D. Remove risk when mitigation results in residual risk within tolerance levels

Answer: C

NEW QUESTION 357
- (Exam Topic 4)
Business management is seeking assurance from the CIO that IT has a plan in place for early identification of potential issues that could impact the delivery of a new application Which of the following is the BEST way to increase the chances of a successful delivery'?

A. Implement a release and deployment plan
B. Conduct comprehensive regression testing.
C. Develop enterprise-wide key risk indicators (KRIs)
D. Include business management on a weekly risk and issues report

Answer: D

NEW QUESTION 361
- (Exam Topic 4)
Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

A. Verifying that project objectives are met
B. Identifying project cost overruns
C. Leveraging an independent review team
D. Reviewing the project initiation risk matrix

Answer: A

NEW QUESTION 362
- (Exam Topic 4)
An organization is planning to move its application infrastructure from on-premises to the cloud. Which of the following is the BEST course of the actin to address the risk associated with data transfer if the relationship is terminated with the vendor?

A. Meet with the business leaders to ensure the classification of their transferred data is in place
B. Ensure the language in the contract explicitly states who is accountable for each step of the data transfer process
C. Collect requirements for the environment to ensure the infrastructure as a service (IaaS) is configured appropriately.
D. Work closely with the information security officer to ensure the company has the proper security controls in place.

Answer: B

NEW QUESTION 364
- (Exam Topic 4)
An incentive program is MOST likely implemented to manage the risk associated with loss of which organizational asset?

A. Employees
B. Data
C. Reputation
D. Customer lists

Answer: A

NEW QUESTION 367
- (Exam Topic 4)
Which of the following is the MOST effective way 10 identify an application backdoor prior to implementation'?

A. User acceptance testing (UAT)
B. Database activity monitoring
C. Source code review
D. Vulnerability analysis

Answer: B

NEW QUESTION 369
- (Exam Topic 4)
Which of the following BEST enables effective IT control implementation?

A. Key risk indicators (KRIs)
B. Documented procedures
C. Information security policies
D. Information security standards

Answer: B

NEW QUESTION 373
- (Exam Topic 4)
An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate tins risk?

A. Requiring the use of virtual private networks (VPNs)
B. Establishing a data classification policy
C. Conducting user awareness training
D. Requiring employee agreement of the acceptable use policy

Answer: C

NEW QUESTION 375
- (Exam Topic 4)
As pan of business continuity planning, which of the following is MOST important to include m a business impact analysis (BIA)?

A. An assessment of threats to the organization
B. An assessment of recovery scenarios
C. industry standard framework
D. Documentation of testing procedures

Answer: A

NEW QUESTION 380
- (Exam Topic 4)
Which of the following is the MOST important course of action for a risk practitioner when reviewing the results of control performance monitoring?

A. Evaluate changes to the organization's risk profile.
B. Validate whether the controls effectively mitigate risk.
C. Confirm controls achieve regulatory compliance.
D. Analyze appropriateness of key performance indicators (KPIs).

Answer: D

NEW QUESTION 384
- (Exam Topic 4)
When preparing a risk status report for periodic review by senior management, it is MOST important to ensure the report includes

A. risk exposure in business terms
B. a detailed view of individual risk exposures
C. a summary of incidents that have impacted the organization.
D. recommendations by an independent risk assessor.

Answer: A

NEW QUESTION 389
- (Exam Topic 4)
The BEST indicator of the risk appetite of an organization is the

A. regulatory environment of the organization
B. risk management capability of the organization
C. board of directors' response to identified risk factors
D. importance assigned to IT in meeting strategic goals

Answer:

B

NEW QUESTION 391
- (Exam Topic 4)
Which of the following would MOST likely require a risk practitioner to update the risk register?

A. An alert being reported by the security operations center.
B. Development of a project schedule for implementing a risk response
C. Completion of a project for implementing a new control
D. Engagement of a third party to conduct a vulnerability scan

Answer: C

NEW QUESTION 395
- (Exam Topic 4)
An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

A. The volume of risk scenarios is too large
B. Risk aggregation has not been completed
C. Risk scenarios are not applicable
D. The risk analysts for each scenario is incomplete

Answer: D

NEW QUESTION 400
- (Exam Topic 4)
One of an organization's key IT systems cannot be patched because the patches interfere with critical business application functionalities. Which of the following would be the risk practitioner's BEST recommendation?

A. Additional mitigating controls should be identified.
B. The system should not be used until the application is changed
C. The organization's IT risk appetite should be adjusted.
D. The associated IT risk should be accepted by management.

Answer: A

NEW QUESTION 403
- (Exam Topic 4)
Which of the following is the PRIMARY reason for an organization to include an acceptable use banner when users log in?

A. To reduce the likelihood of insider threat
B. To eliminate the possibility of insider threat
C. To enable rapid discovery of insider threat
D. To reduce the impact of insider threat

Answer: A

NEW QUESTION 405
- (Exam Topic 4)
Which of the following would BEST mitigate an identified risk scenario?

A. Conducting awareness training
B. Executing a risk response plan
C. Establishing an organization's risk tolerance
D. Performing periodic audits

Answer: C

NEW QUESTION 408
- (Exam Topic 4)
A global organization has implemented an application that does not address all privacy requirements across multiple jurisdictions. Which of the following risk responses has the organization adopted with regard to privacy requirements?

A. Risk avoidance
B. Risk transfer
C. Risk mitigation
D. Risk acceptance

Answer: A

NEW QUESTION 411
- (Exam Topic 4)
Which of the following is the BEST control to minimize the risk associated with scope creep in software development?

A. An established process for project change management

B. Retention of test data and results for review purposes
C. Business managements review of functional requirements
D. Segregation between development, test, and production

Answer: A

NEW QUESTION 412
- (Exam Topic 4)
An organization wants to launch a campaign to advertise a new product Using data analytics, the campaign can be targeted to reach potential customers. Which of the following should be of GREATEST concern to the risk practitioner?

A. Data minimization
B. Accountability
C. Accuracy
D. Purpose limitation

Answer: D

NEW QUESTION 414
- (Exam Topic 4)
Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

A. Verify authorization by senior management.
B. Increase the risk appetite to align with the current risk level
C. Ensure the acceptance is set to expire over lime
D. Update the risk response in the risk register.

Answer: A

NEW QUESTION 415
- (Exam Topic 4)
Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

A. Implement user access controls
B. Perform regular internal audits
C. Develop and communicate fraud prevention policies
D. Conduct fraud prevention awareness training.

Answer: A

NEW QUESTION 420
- (Exam Topic 4)
An organization control environment is MOST effective when:

A. control designs are reviewed periodically
B. controls perform as intended.
C. controls are implemented consistently.
D. controls operate efficiently

Answer: B

NEW QUESTION 425
- (Exam Topic 4)
An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

A. Identify the regulatory bodies that may highlight this gap
B. Highlight news articles about data breaches
C. Evaluate the risk as a measure of probable loss
D. Verify if competitors comply with a similar policy

Answer: B

NEW QUESTION 426
- (Exam Topic 4)
Which of the following is the BEST method to mitigate the risk of an unauthorized employee viewing confidential data in a database''

A. Implement role-based access control
B. Implement a data masking process
C. Include sanctions in nondisclosure agreements (NDAs)
D. Install a data loss prevention (DLP) tool

Answer: A

NEW QUESTION 427

- (Exam Topic 4)
Which of the following is MOST helpful in identifying loss magnitude during risk analysis of a new system?

A. Recovery time objective (RTO)
B. Cost-benefit analysis
C. Business impact analysis (BIA)
D. Cyber insurance coverage

Answer: C

NEW QUESTION 430
- (Exam Topic 4)
An organization's recovery team is attempting to recover critical data backups following a major flood in its data center. However, key team members do not know exactly what steps should be taken to address this crisis. Which of the following is the MOST likely cause of this situation?

A. Failure to test the disaster recovery plan (DRP)
B. Lack of well-documented business impact analysis (BIA)
C. Lack of annual updates to the disaster recovery plan (DRP)
D. Significant changes in management personnel

Answer: A

NEW QUESTION 435
- (Exam Topic 4)
An organization plans to implement a new Software as a Service (SaaS) speech-to-text solution Which of the following is MOST important to mitigate risk associated with data privacy?

A. Secure encryption protocols are utilized.
B. Multi-factor authentication is set up for users.
C. The solution architecture is approved by IT.
D. A risk transfer clause is included in the contact

Answer: A

NEW QUESTION 439
- (Exam Topic 4)
A risk practitioner observed Vial a high number of pokey exceptions were approved by senior management. Which of the following is the risk practitioner's BEST course of action to determine root cause?

A. Review the risk profile
B. Review pokey change history
C. interview the control owner
D. Perform control testing

Answer: C

NEW QUESTION 441
- (Exam Topic 4)
An organization has experienced a cyber attack that exposed customer personally identifiable information (Pll) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

A. Security control owners based on control failures
B. Cyber risk remediation plan owners
C. Risk owners based on risk impact
D. Enterprise risk management (ERM) team

Answer: C

NEW QUESTION 443
- (Exam Topic 4)
Which of the following is the GREATEST benefit of centralizing IT systems?

A. Risk reporting
B. Risk classification
C. Risk monitoring
D. Risk identification

Answer: C

NEW QUESTION 448
- (Exam Topic 4)
An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?

A. Acquisition
B. Implementation
C. Initiation

D. Operation and maintenance

Answer: C

NEW QUESTION 452
- (Exam Topic 4)
An organization has experienced several incidents of extended network outages that have exceeded tolerance. Which of the following should be the risk practitioner's FIRST step to address this situation?

A. Recommend additional controls to address the risk.
B. Update the risk tolerance level to acceptable thresholds.
C. Update the incident-related risk trend in the risk register.
D. Recommend a root cause analysis of the incidents.

Answer: D

NEW QUESTION 456
- (Exam Topic 4)
Which of the following is MOST important for successful incident response?

A. The quantity of data logged by the attack control tools
B. Blocking the attack route immediately
C. The ability to trace the source of the attack
D. The timeliness of attack recognition

Answer: D

NEW QUESTION 458
- (Exam Topic 4)
Which of the following BEST helps to identify significant events that could impact an organization?

A. Control analysis
B. Vulnerability analysis
C. Scenario analysis
D. Heat map analysis

Answer: C

NEW QUESTION 462
- (Exam Topic 4)
A risk practitioner is reviewing accountability assignments for data risk in the risk register. Which of the following would pose the GREATEST concern?

A. The risk owner is not the control owner for associated data controls.
B. The risk owner is in a business unit and does not report through the IT department.
C. The risk owner is listed as the department responsible for decision making.
D. The risk owner is a staff member rather than a department manager.

Answer: C

NEW QUESTION 466
- (Exam Topic 4)
Which of the following will BEST help to ensure implementation of corrective action plans?

A. Establishing employee awareness training
B. Assigning accountability to risk owners
C. Selling target dates to complete actions
D. Contracting to third parties

Answer: B

NEW QUESTION 471
- (Exam Topic 4)
Which of the following is the BEST approach for selecting controls to minimize risk?

A. Industry best practice review
B. Risk assessment
C. Cost-benefit analysis
D. Control-effectiveness evaluation

Answer: C

NEW QUESTION 476
- (Exam Topic 4)
Which of the following provides the MOST reliable evidence of a control's effectiveness?

A. A risk and control self-assessment
B. Senior management's attestation
C. A system-generated testing report
D. detailed process walk-through

Answer: D

NEW QUESTION 479
- (Exam Topic 4)
Which of the following is the PRIMARY objective of establishing an organization's risk tolerance and appetite?

A. To align with board reporting requirements
B. To assist management in decision making
C. To create organization-wide risk awareness
D. To minimize risk mitigation efforts

Answer: B

NEW QUESTION 481
- (Exam Topic 4)
Which of the following is MOST important to include when reporting the effectiveness of risk management to senior management?

A. Changes in the organization's risk appetite and risk tolerance levels
B. Impact due to changes in external and internal risk factors
C. Changes in residual risk levels against acceptable levels
D. Gaps in best practices and implemented controls across the industry

Answer: C

NEW QUESTION 484
- (Exam Topic 4)
Which of the following is MOST important to update when an organization's risk appetite changes?

A. Key risk indicators (KRIs)
B. Risk reporting methodology
C. Key performance indicators (KPIs)
D. Risk taxonomy

Answer: A

NEW QUESTION 488
- (Exam Topic 4)
Which key performance efficiency IKPI) BEST measures the effectiveness of an organization's disaster recovery program?

A. Number of service level agreement (SLA) violations
B. Percentage of recovery issues identified during the exercise
C. Number of total systems recovered within tie recovery point objective (RPO)
D. Percentage of critical systems recovered within tie recovery time objective (RTO)

Answer: D

NEW QUESTION 490
- (Exam Topic 4)
After an annual risk assessment is completed, which of the following would be MOST important to communicate to stakeholders?

A. A decrease in threats
B. A change in the risk profile
C. An increase in reported vulnerabilities
D. An increase in identified risk scenarios

Answer: B

NEW QUESTION 492
- (Exam Topic 4)
Which of the following would be the GREATEST concern for an IT risk practitioner when an employees.....

A. The organization's structure has not been updated
B. Unnecessary access permissions have not been removed.
C. Company equipment has not been retained by IT
D. Job knowledge was not transferred to employees m the former department

Answer: B

NEW QUESTION 494
- (Exam Topic 4)

Which of the following is the MOST useful information for a risk practitioner when planning response activities after risk identification?

A. Risk register
B. Risk appetite
C. Risk priorities
D. Risk heat maps

Answer: B

NEW QUESTION 496
- (Exam Topic 4)
It is MOST important that security controls for a new system be documented in:

A. testing requirements
B. the implementation plan.
C. System requirements
D. The security policy

Answer: C

NEW QUESTION 501
- (Exam Topic 4)
Which of the following is the GREATEST benefit of identifying appropriate risk owners?

A. Accountability is established for risk treatment decisions
B. Stakeholders are consulted about risk treatment options
C. Risk owners are informed of risk treatment options
D. Responsibility is established for risk treatment decisions.

Answer: A

NEW QUESTION 506
- (Exam Topic 4)
Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

A. To identify gaps in data protection controls
B. To develop a customer notification plan
C. To identify personally identifiable information (PII)
D. To determine gaps in data identification processes

Answer: A

NEW QUESTION 508
- (Exam Topic 4)
Which of the following is the GREATEST benefit of a three lines of defense structure?

A. An effective risk culture that empowers employees to report risk
B. Effective segregation of duties to prevent internal fraud
C. Clear accountability for risk management processes
D. Improved effectiveness and efficiency of business operations

Answer: C

NEW QUESTION 513
- (Exam Topic 4)
A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

A. Risk manager
B. Control owner
C. Control tester
D. Risk owner

Answer: B

NEW QUESTION 516
- (Exam Topic 4)
Which of the following should be the PRIMARY input to determine risk tolerance?

A. Regulatory requirements
B. Organizational objectives
C. Annual loss expectancy (ALE)
D. Risk management costs

Answer: C

NEW QUESTION 520
- (Exam Topic 4)
Which of the following will BEST ensure that controls adequately support business goals and objectives?

A. Using the risk management process
B. Enforcing strict disciplinary procedures in case of noncompliance
C. Reviewing results of the annual company external audit
D. Adopting internationally accepted controls

Answer: A

NEW QUESTION 522
- (Exam Topic 4)
Which of the following would MOST effectively reduce risk associated with an increase of online transactions on a retailer website?

A. Scalable infrastructure
B. A hot backup site
C. Transaction limits
D. Website activity monitoring

Answer: C

NEW QUESTION 523
- (Exam Topic 4)
Which of the following is the MOST important benefit of reporting risk assessment results to senior management?

A. Promotion of a risk-aware culture
B. Compilation of a comprehensive risk register
C. Alignment of business activities
D. Facilitation of risk-aware decision making

Answer: D

NEW QUESTION 527
- (Exam Topic 3)
Which of the following should be implemented to BEST mitigate the risk associated with infrastructure updates?

A. Role-specific technical training
B. Change management audit
C. Change control process
D. Risk assessment

Answer: C

NEW QUESTION 528
- (Exam Topic 3)
A risk practitioner has just learned about new malware that has severely impacted industry peers worldwide data loss?

A. Customer database manager
B. Customer data custodian
C. Data privacy officer
D. Audit committee

Answer: B

NEW QUESTION 533
- (Exam Topic 3)
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual
risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

A. Identify new risk entries to include in ERM.
B. Remove the risk entries from the ERM register.
C. Re-perform the risk assessment to confirm results.
D. Verify the adequacy of risk monitoring plans.

Answer: D

NEW QUESTION 536
- (Exam Topic 3)
To minimize the risk of a potential acquisition being exposed externally, an organization has selected a few
key employees to be engaged in the due diligence process. A member of the due diligence team realizes a close acquaintance is a high-ranking IT professional at a subsidiary of the company about to be acquired. What is the BEST course of action for this team member?

A. Enforce segregation of duties.
B. Disclose potential conflicts of interest.
C. Delegate responsibilities involving the acquaintance.
D. Notify the subsidiary's legal team.

Answer: B

NEW QUESTION 537
- (Exam Topic 3)
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: A

NEW QUESTION 538
- (Exam Topic 3)
Which of the following would BEST mitigate the risk associated with reputational damage from inappropriate use of social media sites by employees?

A. Validating employee social media accounts and passwords
B. Monitoring Internet usage on employee workstations
C. Disabling social media access from the organization's technology
D. Implementing training and awareness programs

Answer: D

NEW QUESTION 543
- (Exam Topic 3)
Which of the following describes the relationship between Key risk indicators (KRIs) and key control indicators (KCIS)?

A. KCIs are independent from KRIs KRIs.
B. KCIs and KRIs help in determining risk appetite.
C. KCIs are defined using data from KRIs.
D. KCIs provide input for KRIs

Answer: D

NEW QUESTION 544
- (Exam Topic 3)
A chief information officer (CIO) has identified risk associated with shadow systems being maintained by business units to address specific functionality gaps in the organization's enterprise resource planning (ERP) system. What is the BEST way to reduce this risk going forward?

A. Align applications to business processes.
B. Implement an enterprise architecture (EA).
C. Define the software development life cycle (SDLC).
D. Define enterprise-wide system procurement requirements.

Answer: B

NEW QUESTION 545
- (Exam Topic 3)
An information system for a key business operation is being moved from an in-house application to a Software as a Service (SaaS) vendor. Which of the following will have the GREATEST impact on the ability to monitor risk?

A. Reduced ability to evaluate key risk indicators (KRIs)
B. Reduced access to internal audit reports
C. Dependency on the vendor's key performance indicators (KPIs)
D. Dependency on service level agreements (SLAs)

Answer: A

NEW QUESTION 547
- (Exam Topic 3)
When an organization’s disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?

A. Acceptance
B. Mitigation
C. Transfer
D. Avoidance

Answer: B

NEW QUESTION 552
- (Exam Topic 3)
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: D

NEW QUESTION 553
- (Exam Topic 3)
A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

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

Answer: D

NEW QUESTION 556
- (Exam Topic 3)
Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

A. Cost of controls
B. Risk tolerance
C. Risk appetite
D. Probability definition

Answer: A

NEW QUESTION 558
- (Exam Topic 3)
Which of the following is the MOST effective control to ensure user access is maintained on a least-privilege basis?

A. User authorization
B. User recertification
C. Change log review
D. Access log monitoring

Answer: B

NEW QUESTION 559
- (Exam Topic 3)
What is the PRIMARY purpose of a business impact analysis (BIA)?

A. To determine the likelihood and impact of threats to business operations
B. To identify important business processes in the organization
C. To estimate resource requirements for related business processes
D. To evaluate the priority of business operations in case of disruption

Answer: D

NEW QUESTION 561
- (Exam Topic 3)
A risk practitioner has been asked by executives to explain how existing risk treatment plans would affect risk posture at the end of the year. Which of the following is MOST helpful in responding to this request?

A. Assessing risk with no controls in place
B. Showing projected residual risk
C. Providing peer benchmarking results
D. Assessing risk with current controls in place

Answer: D

NEW QUESTION 563

- (Exam Topic 3)
An organization planning to transfer and store its customer data with an offshore cloud service provider should be PRIMARILY concerned with:

A. data aggregation
B. data privacy
C. data quality
D. data validation

Answer: B

NEW QUESTION 566
- (Exam Topic 3)
Prudent business practice requires that risk appetite not exceed:

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

Answer: C

NEW QUESTION 570
- (Exam Topic 3)
Which of the following is the STRONGEST indication an organization has ethics management issues?

A. Employees do not report IT risk issues for fear of consequences.
B. Internal IT auditors report to the chief information security officer (CISO).
C. Employees face sanctions for not signing the organization's acceptable use policy.
D. The organization has only two lines of defense.

Answer: A

NEW QUESTION 574
- (Exam Topic 3)
After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?

A. Obtain industry benchmarks related to the specific risk.
B. Provide justification for the lower risk rating.
C. Notify the business at the next risk briefing.
D. Reopen the risk issue and complete a full assessment.

Answer: B

NEW QUESTION 575
- (Exam Topic 3)
Which of the following provides the BEST measurement of an organization's risk management maturity level?

A. Level of residual risk
B. The results of a gap analysis
C. IT alignment to business objectives
D. Key risk indicators (KRIs)

Answer: C

NEW QUESTION 577
- (Exam Topic 3)
An organization's IT infrastructure is running end-of-life software that is not allowed without exception approval. Which of the following would provide the MOST helpful information to justify investing in updated software?

A. The balanced scorecard
B. A cost-benefit analysis
C. The risk management frameworkD, A roadmap of IT strategic planning

Answer: B

NEW QUESTION 579
- (Exam Topic 3)
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: A

NEW QUESTION 584
- (Exam Topic 3)
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 589
- (Exam Topic 3)
The BEST indication that risk management is effective is when risk has been reduced to meet:

A. risk levels.
B. risk budgets.
C. risk appetite.
D. risk capacity.

Answer: C

NEW QUESTION 591
- (Exam Topic 3)
Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

A. Improved senior management communication
B. Optimized risk treatment decisions
C. Enhanced awareness of risk management
D. Improved collaboration among risk professionals

Answer: B

NEW QUESTION 596
- (Exam Topic 3)
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 598
- (Exam Topic 3)
Which of the following is MOST important when developing risk scenarios?

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

Answer: D

NEW QUESTION 600
- (Exam Topic 3)
Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?

A. Develop a risk treatment plan.
B. Validate organizational risk appetite.
C. Review results of prior risk assessments.
D. Include the current and desired states in the risk register.

Answer: A

NEW QUESTION 605
- (Exam Topic 3)
A maturity model is MOST useful to an organization when it:

A. benchmarks against other organizations
B. defines a qualitative measure of risk
C. provides a reference for progress
D. provides risk metrics.

Answer: C

NEW QUESTION 610
- (Exam Topic 3)
Which of the following will BEST help in communicating strategic risk priorities?

A. Heat map
B. Business impact analysis (BIA)
C. Balanced Scorecard
D. Risk register

Answer: A

NEW QUESTION 614
- (Exam Topic 3)
Which of the following is the PRIMARY reason to adopt key control indicators (KCIs) in the risk monitoring and reporting process?

A. To provide data for establishing the risk profile
B. To provide assurance of adherence to risk management policies
C. To provide measurements on the potential for risk to occur
D. To provide assessments of mitigation effectiveness

Answer: D

NEW QUESTION 618
- (Exam Topic 3)
A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:

A. management.
B. tolerance.
C. culture.
D. analysis.

Answer: C

NEW QUESTION 619
- (Exam Topic 3)
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 622
- (Exam Topic 3)
Which of me following is MOST helpful to mitigate the risk associated with an application under development not meeting business objectives?

A. Identifying tweets that may compromise enterprise architecture (EA)
B. Including diverse Business scenarios in user acceptance testing (UAT)
C. Performing risk assessments during the business case development stage
D. Including key stakeholders in review of user requirements

Answer: D

NEW QUESTION 626
- (Exam Topic 3)
The GREATEST benefit of including low-probability, high-impact events in a risk assessment is the ability to:

A. develop a comprehensive risk mitigation strategy
B. develop understandable and realistic risk scenarios
C. identify root causes for relevant events
D. perform an aggregated cost-benefit analysis

Answer: D

NEW QUESTION 629
- (Exam Topic 3)
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 634
- (Exam Topic 3)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an antivirus program?

A. Percentage of IT assets with current malware definitions
B. Number of false positives defected over a period of time
C. Number of alerts generated by the anti-virus software
D. Frequency of anti-vinjs software updates

Answer: A

NEW QUESTION 636
- (Exam Topic 3)
An organization is implementing encryption for data at rest to reduce the risk associated with unauthorized access. Which of the following MUST be considered to assess the residual risk?

A. Data retention requirements
B. Data destruction requirements
C. Cloud storage architecture
D. Key management

Answer: D

NEW QUESTION 637
- (Exam Topic 3)
When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction based on:

A. cost-benefit analysis.
B. risk appetite.
C. regulatory guidelines
D. control efficiency

Answer: A

NEW QUESTION 642
- (Exam Topic 3)
Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

A. Control self-assessment (CSA)
B. Security information and event management (SIEM) solutions
C. Data privacy impact assessment (DPIA)
D. Data loss prevention (DLP) tools

Answer: B

NEW QUESTION 647
- (Exam Topic 3)
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: B

NEW QUESTION 649
- (Exam Topic 3)
The MOST important consideration when selecting a control to mitigate an identified risk is whether:

A. the cost of control exceeds the mitigation value
B. there are sufficient internal resources to implement the control
C. the mitigation measures create compounding effects
D. the control eliminates the risk

Answer: A

NEW QUESTION 654
- (Exam Topic 3)
Which of the following presents the GREATEST risk to change control in business application development over the complete life cycle?

A. Emphasis on multiple application testing cycles
B. Lack of an integrated development environment (IDE) tool
C. Introduction of requirements that have not been approved
D. Bypassing quality requirements before go-live

Answer: C

NEW QUESTION 656
- (Exam Topic 3)
Which of the following MUST be updated to maintain an IT risk register?

A. Expected frequency and potential impact
B. Risk tolerance
C. Enterprise-wide IT risk assessment
D. Risk appetite

Answer: C

NEW QUESTION 659
- (Exam Topic 3)
While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially Which of the following would be the BEST approach for the risk practitioner to take?

A. Temporarily suspend emergency changes.
B. Document the control deficiency in the risk register.
C. Conduct a root cause analysis.
D. Continue monitoring change management metrics.

Answer: C

NEW QUESTION 664
- (Exam Topic 3)
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: A

NEW QUESTION 669
- (Exam Topic 3)
Accountability for a particular risk is BEST represented in a:

A. risk register
B. risk catalog
C. risk scenario
D. RACI matrix

Answer: D

NEW QUESTION 671
- (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 674
- (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 675

- (Exam Topic 2)
The PRIMARY reason for establishing various Threshold levels for a set of key risk indicators (KRIs) is to:

A. highlight trends of developing risk.
B. ensure accurate and reliable monitoring.
C. take appropriate actions in a timely manner.
D. set different triggers for each stakeholder.

Answer: B

NEW QUESTION 679
- (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: D

NEW QUESTION 683
- (Exam Topic 2)
The PRIMARY objective of The board of directors periodically reviewing the risk profile is to help ensure:

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

Answer: A

NEW QUESTION 685
- (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: A

NEW QUESTION 687
- (Exam Topic 2)
An organization's risk practitioner learns a new third-party system on the corporate network has introduced vulnerabilities that could compromise corporate IT systems. What should the risk practitioner do
FIRST?

A. Confirm the vulnerabilities with the third party
B. Identify procedures to mitigate the vulnerabilities.
C. Notify information security management.
D. Request IT to remove the system from the network.

Answer: B

NEW QUESTION 691
- (Exam Topic 2)
Which of the following is a crucial component of a key risk indicator (KRI) to ensure appropriate action is taken to mitigate risk?

A. Management intervention
B. Risk appetite
C. Board commentary
D. Escalation triggers

Answer: D

NEW QUESTION 695
- (Exam Topic 2)
Which of the following MUST be assessed before considering risk treatment options for a scenario with significant impact?

A. Risk magnitude
B. Incident probability
C. Risk appetite
D. Cost-benefit analysis

Answer: D

NEW QUESTION 697
- (Exam Topic 2)
Which of the following is MOST important when defining controls?

A. Identifying monitoring mechanisms
B. Including them in the risk register
C. Aligning them with business objectives
D. Prototyping compensating controls

Answer: C

NEW QUESTION 699
- (Exam Topic 2)
Who is accountable for risk treatment?

A. Enterprise risk management team
B. Risk mitigation manager
C. Business process owner
D. Risk owner

Answer: D

NEW QUESTION 704
- (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 707
- (Exam Topic 2)
Which of the following could BEST detect an in-house developer inserting malicious functions into a web-based application?

A. Segregation of duties
B. Code review
C. Change management
D. Audit modules

Answer: B

NEW QUESTION 712
- (Exam Topic 2)
After identifying new risk events during a project, the project manager s NEXT step should be to:

A. determine if the scenarios need 10 be accepted or responded to.
B. record the scenarios into the risk register.
C. continue with a qualitative risk analysis.
D. continue with a quantitative risk analysis.

Answer: B

NEW QUESTION 717
- (Exam Topic 2)
Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?

A. Audit and compliance management
B. The chief information officer (CIO) and the chief financial officer (CFO)
C. Enterprise risk management and business process owners
D. Executive management and the board of directors

Answer: D

NEW QUESTION 722
- (Exam Topic 2)
The BEST way to test the operational effectiveness of a data backup procedure is to:

A. conduct an audit of files stored offsite.
B. interview employees to compare actual with expected procedures.
C. inspect a selection of audit trails and backup logs.
D. demonstrate a successful recovery from backup files.

Answer: D

NEW QUESTION 724
- (Exam Topic 2)
Which of the following resources is MOST helpful when creating a manageable set of IT risk scenarios?

A. Results of current and past risk assessments
B. Organizational strategy and objectives
C. Lessons learned from materialized risk scenarios
D. Internal and external audit findings

Answer: B

NEW QUESTION 729
- (Exam Topic 2)
Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?

A. Facilitating risk-aware decision making by stakeholders
B. Demonstrating management commitment to mitigate risk
C. Closing audit findings on a timely basis
D. Ensuring compliance to industry standards

Answer: A

NEW QUESTION 734
- (Exam Topic 2)
Which of the following conditions presents the GREATEST risk to an application?

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

Answer: D

NEW QUESTION 736
- (Exam Topic 2)
What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

A. Risk and control ownership
B. Senior management participation
C. Business unit support
D. Risk nomenclature and taxonomy

Answer: B

NEW QUESTION 737
- (Exam Topic 2)
An organization is considering modifying its system to enable acceptance of credit card payments. To reduce the risk of data exposure, which of the following should the organization do FIRST?

A. Conduct a risk assessment.
B. Update the security strategy.
C. Implement additional controls.
D. Update the risk register.

Answer: A

NEW QUESTION 741
- (Exam Topic 2)
An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Alpha	High	Medium	High
Bravo	High	Low	Medium
Charlie	High	High	High
Delta	High	Medium	Medium

A. Project Charlie
B. Project Bravo
C. Project Alpha
D. Project Delta

Answer: A

NEW QUESTION 744
- (Exam Topic 2)
Which of the following is the PRIMARY reason to establish the root cause of an IT security incident?

A. Update the risk register.
B. Assign responsibility and accountability for the incident.
C. Prepare a report for senior management.
D. Avoid recurrence of the incident.

Answer: D

NEW QUESTION 747
- (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 750
- (Exam Topic 2)
A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

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

Answer: A

NEW QUESTION 755
- (Exam Topic 2)
Which of these documents is MOST important to request from a cloud service provider during a vendor risk assessment?

A. Nondisclosure agreement (NDA)
B. Independent audit report
C. Business impact analysis (BIA)
D. Service level agreement (SLA)

Answer: B

NEW QUESTION 756
- (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 761
- (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: A

NEW QUESTION 764
- (Exam Topic 2)
Which of the following BEST enables the risk profile to serve as an effective resource to support business objectives?

A. Engaging external risk professionals to periodically review the risk
B. Prioritizing global standards over local requirements in the risk profile
C. Updating the risk profile with risk assessment results

D. Assigning quantitative values to qualitative metrics in the risk register

Answer: C

NEW QUESTION 765
- (Exam Topic 2)
Which of the following provides the BEST evidence that risk responses have been executed according to their risk action plans?

A. Risk policy review
B. Business impact analysis (B1A)
C. Control catalog
D. Risk register

Answer: D

NEW QUESTION 769
- (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 771
- (Exam Topic 2)
An organization's risk tolerance should be defined and approved by which of the following?

A. The chief risk officer (CRO)
B. The board of directors
C. The chief executive officer (CEO)
D. The chief information officer (CIO)

Answer: B

NEW QUESTION 773
- (Exam Topic 2)
Which of the following is MOST likely to be impacted as a result of a new policy which allows staff members to remotely connect to the organization's IT systems via personal or public computers?

A. Risk appetite
B. Inherent risk
C. Key risk indicator (KRI)
D. Risk tolerance

Answer: B

NEW QUESTION 776
- (Exam Topic 2)
The MAIN purpose of a risk register is to:

A. document the risk universe of the organization.
B. promote an understanding of risk across the organization.
C. enable well-informed risk management decisions.
D. identify stakeholders associated with risk scenarios.

Answer: C

NEW QUESTION 780
- (Exam Topic 2)
The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

A. ensure policy and regulatory compliance.
B. assess the proliferation of new threats.

C. verify Internet firewall control settings.
D. identify vulnerabilities in the system.

Answer: C

NEW QUESTION 781
- (Exam Topic 2)
A new policy has been published to forbid copying of data onto removable media. Which type of control has been implemented?

A. Preventive
B. Detective
C. Directive
D. Deterrent

Answer: C

NEW QUESTION 785
- (Exam Topic 2)
The annualized loss expectancy (ALE) method of risk analysis:

A. helps in calculating the expected cost of controls
B. uses qualitative risk rankings such as lo
C. medium and high.
D. can be used m a cost-benefit analysts
E. can be used to determine the indirect business impact.

Answer: C

NEW QUESTION 786
- (Exam Topic 2)
An IT operations team implements disaster recovery controls based on decisions from application owners regarding the level of resiliency needed. Who is the risk owner in this scenario?

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

Answer: C

NEW QUESTION 788
- (Exam Topic 2)
Which of the following should an organization perform to forecast the effects of a disaster?

A. Develop a business impact analysis (BIA).
B. Define recovery time objectives (RTO).
C. Analyze capability maturity model gaps.
D. Simulate a disaster recovery.

Answer: A

NEW QUESTION 789
- (Exam Topic 2)
A risk practitioner recently discovered that sensitive data from the production environment is required for testing purposes in non-production environments. Which of the following i the BEST recommendation to address this situation?

A. Enable data encryption in the test environment
B. Implement equivalent security in the test environment.
C. Prevent the use of production data for test purposes
D. Mask data before being transferred to the test environment.

Answer: B

NEW QUESTION 792
- (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 795

- (Exam Topic 2)
Which of the following is MOST helpful to review when identifying risk scenarios associated with the adoption of Internet of Things (IoT) technology in an organization?

A. The business case for the use of IoT
B. The IoT threat landscape
C. Policy development for IoT
D. The network that IoT devices can access

Answer: B

NEW QUESTION 798
- (Exam Topic 2)
Reviewing which of the following provides the BEST indication of an organizations risk tolerance?

A. Risk sharing strategy
B. Risk transfer agreements
C. Risk policies
D. Risk assessments

Answer: D

NEW QUESTION 799
- (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: D

NEW QUESTION 803
- (Exam Topic 2)
Which of the following would be MOST beneficial as a key risk indicator (KRI)?

A. Current capital allocation reserves
B. Negative security return on investment (ROI)
C. Project cost variances
D. Annualized loss projections

Answer: D

NEW QUESTION 804
- (Exam Topic 2)
Which of the following should a risk practitioner do FIRST when an organization decides to use a cloud service?

A. Review the vendor selection process and vetting criteria.
B. Assess whether use of service falls within risk tolerance thresholds.
C. Establish service level agreements (SLAs) with the vendor.
D. Check the contract for appropriate security risk and control provisions.

Answer: D

NEW QUESTION 807
- (Exam Topic 2)
A risk assessment indicates the residual risk associated with a new bring your own device (BYOD) program is within organizational risk tolerance. Which of the following should the risk practitioner
recommend be done NEXT?

A. Implement targeted awareness training for new BYOD users.
B. Implement monitoring to detect control deterioration.
C. Identify log sources to monitor BYOD usage and risk impact.
D. Reduce the risk tolerance level.

Answer: B

NEW QUESTION 808
- (Exam Topic 2)
Which of the following is the MOST important input when developing risk scenarios?

A. Key performance indicators
B. Business objectives
C. The organization's risk framework
D. Risk appetite

Answer: B

NEW QUESTION 810
- (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 812
- (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 816
- (Exam Topic 2)
When establishing leading indicators for the information security incident response process it is MOST important to consider the percentage of reported incidents:

A. that result in a full root cause analysis.
B. used for verification within the SLA.
C. that are verified as actual incidents.
D. resolved within the SLA.

Answer: C

NEW QUESTION 817
- (Exam Topic 2)
Which of the following is the BEST way to identify changes in the risk profile of an organization?

A. Monitor key risk indicators (KRIs).
B. Monitor key performance indicators (KPIs).
C. Interview the risk owner.
D. Conduct a gap analysis

Answer: D

NEW QUESTION 822
- (Exam Topic 2)
The maturity of an IT risk management program is MOST influenced by:

A. the organization's risk culture
B. benchmarking results against similar organizations
C. industry-specific regulatory requirements
D. expertise available within the IT department

Answer: A

NEW QUESTION 826
- (Exam Topic 2)
Which of the following is MOST helpful in identifying gaps between the current and desired state of the IT risk environment?

A. Analyzing risk appetite and tolerance levels
B. Assessing identified risk and recording results in the risk register
C. Evaluating risk scenarios and assessing current controls
D. Reviewing guidance from industry best practices and standards

Answer: C

NEW QUESTION 828
- (Exam Topic 2)
Which of the following would MOST likely result in updates to an IT risk appetite statement?

A. External audit findings
B. Feedback from focus groups
C. Self-assessment reports

D. Changes in senior management

Answer: D

NEW QUESTION 830
- (Exam Topic 2)
A risk practitioner notices a trend of noncompliance with an IT-related control. Which of the following would BEST assist in making a recommendation to management?

A. Assessing the degree to which the control hinders business objectives
B. Reviewing the IT policy with the risk owner
C. Reviewing the roles and responsibilities of control process owners
D. Assessing noncompliance with control best practices

Answer: A

NEW QUESTION 835
- (Exam Topic 2)
Which of the following is the MOST important objective of embedding risk management practices into the initiation phase of the project management life cycle?

A. To deliver projects on time and on budget
B. To assess inherent risk
C. To include project risk in the enterprise-wide IT risk profit.
D. To assess risk throughout the project

Answer: B

NEW QUESTION 838
- (Exam Topic 2)
An organization has outsourced its backup and recovery procedures to a third-party cloud provider. Which of the following is the risk practitioner s BEST course of action?

A. Accept the risk and document contingency plans for data disruption.
B. Remove the associated risk scenario from the risk register due to avoidance.
C. Mitigate the risk with compensating controls enforced by the third-party cloud provider.
D. Validate the transfer of risk and update the register to reflect the change.

Answer: C

NEW QUESTION 840
- (Exam Topic 2)
Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

A. Cyber insurance
B. Data backups
C. Incident response plan
D. Key risk indicators (KRIs)

Answer: D

NEW QUESTION 842
- (Exam Topic 2)
An organization has implemented a system capable of comprehensive employee monitoring. Which of the following should direct how the system is used?

A. Organizational strategy
B. Employee code of conduct
C. Industry best practices
D. Organizational policy

Answer: D

NEW QUESTION 847
- (Exam Topic 2)
Which of the following would BEST enable a risk practitioner to embed risk management within the organization?

A. Provide risk management feedback to key stakeholders.
B. Collect and analyze risk data for report generation.
C. Monitor and prioritize risk data according to the heat map.
D. Engage key stakeholders in risk management practices.

Answer: D

NEW QUESTION 849
- (Exam Topic 2)

Which of the following is the PRIMARY benefit of identifying and communicating with stakeholders at the onset of an IT risk assessment?

A. Obtaining funding support
B. Defining the risk assessment scope
C. Selecting the risk assessment framework
D. Establishing inherent risk

Answer: B

NEW QUESTION 852
- (Exam Topic 2)
Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

A. Self-assessment questionnaires completed by management
B. Review of internal audit and third-party reports
C. Management review and sign-off on system documentation
D. First-hand direct observation of the controls in operation

Answer: B

NEW QUESTION 857
- (Exam Topic 2)
A business unit has decided to accept the risk of implementing an off-the-shelf, commercial software package that uses weak password controls. The BEST course of action would be to:

A. obtain management approval for policy exception.
B. develop an improved password software routine.
C. select another application with strong password controls.
D. continue the implementation with no changes.

Answer: B

NEW QUESTION 861
- (Exam Topic 2)
An organization has received notification that it is a potential victim of a cybercrime that may have compromised sensitive customer data. What should be The FIRST course of action?

A. Invoke the incident response plan.
B. Determine the business impact.
C. Conduct a forensic investigation.
D. Invoke the business continuity plan (BCP).

Answer: A

NEW QUESTION 866
- (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: B

NEW QUESTION 868
- (Exam Topic 2)
The PRIMARY purpose of vulnerability assessments is to:

A. provide clear evidence that the system is sufficiently secure.
B. determine the impact of potential threats.
C. test intrusion detection systems (IDS) and response procedures.
D. detect weaknesses that could lead to system compromise.

Answer: D

NEW QUESTION 872
- (Exam Topic 2)
Which of the following provides The MOST useful information when determining a risk management program's maturity level?

A. Risk assessment results
B. A recently reviewed risk register
C. Key performance indicators (KPIs)
D. The organization's risk framework

Answer: A

NEW QUESTION 876
- (Exam Topic 2)
Which of the following is the GREATEST concern when an organization uses a managed security service provider as a firewall administrator?

A. Exposure of log data
B. Lack of governance
C. Increased number of firewall rules
D. Lack of agreed-upon standards

Answer: B

NEW QUESTION 877
- (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 878
- (Exam Topic 2)
Which of the following is MOST important to enable well-informed cybersecurity risk decisions?

A. Determine and understand the risk rating of scenarios.
B. Conduct risk assessment peer reviews.
C. Identify roles and responsibilities for security controls.
D. Engage a third party to perform a risk assessment.

Answer: A

NEW QUESTION 881
- (Exam Topic 2)
The MAIN purpose of having a documented risk profile is to:

A. comply with external and internal requirements.
B. enable well-informed decision making.
C. prioritize investment projects.
D. keep the risk register up-to-date.

Answer: B

NEW QUESTION 884
- (Exam Topic 2)
A bank has outsourced its statement printing function to an external service provider. Which of the following is the MOST critical requirement to include in the contract?

A. Monitoring of service costs
B. Provision of internal audit reports
C. Notification of sub-contracting arrangements
D. Confidentiality of customer data

Answer: D

NEW QUESTION 888
- (Exam Topic 2)
A payroll manager discovers that fields in certain payroll reports have been modified without authorization. Which of the following control weaknesses could have contributed MOST to this problem?

A. The user requirements were not documented.
B. Payroll files were not under the control of a librarian.
C. The programmer had access to the production programs.
D. The programmer did not involve the user in testing.

Answer: B

NEW QUESTION 893
- (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 898
- (Exam Topic 2)
Which of the following activities should be performed FIRST when establishing IT risk management processes?

A. Collect data of past incidents and lessons learned.
B. Conduct a high-level risk assessment based on the nature of business.
C. Identify the risk appetite of the organization.
D. Assess the goals and culture of the organization.

Answer: D

NEW QUESTION 903
.....

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