Exam Questions CRISC

Certified in Risk and Information Systems Control

https://www.2passeasy.com/dumps/CRISC/

NEW QUESTION 1
- (Exam Topic 4)
When classifying and prioritizing risk responses, the areas to address FIRST are those with:

A. low cost effectiveness ratios and high risk levels
B. high cost effectiveness ratios and low risk levels.
C. high cost effectiveness ratios and high risk levels
D. low cost effectiveness ratios and low risk levels.

Answer: C

NEW QUESTION 2
- (Exam Topic 4)
Which of the following should be the GREATEST concern to a risk practitioner when process documentation is incomplete?

A. Inability to allocate resources efficiently
B. Inability to identify the risk owner
C. Inability to complete the risk register
D. Inability to identify process experts

Answer: B

NEW QUESTION 3
- (Exam Topic 4)
A global company s business continuity plan (BCP) requires the transfer of its customer information…. event of a disaster. Which of the following should be the MOST important risk consideration?

A. The difference In the management practices between each company
B. The cloud computing environment is shared with another company
C. The lack of a service level agreement (SLA) in the vendor contract
D. The organizational culture differences between each country

Answer: B

NEW QUESTION 4
- (Exam Topic 4)
Which of the following is the PRIMARY accountability for a control owner?

A. Communicate risk to senior management.
B. Own the associated risk the control is mitigating.
C. Ensure the control operates effectively.
D. Identify and assess control weaknesses.

Answer: C

NEW QUESTION 5
- (Exam Topic 4)
An organization's business gap analysis reveals the need for a robust IT risk strategy. Which of the following should be the risk practitioner's PRIMARY consideration when participating in development of the new strategy?

A. Scale of technology
B. Risk indicators
C. Risk culture
D. Proposed risk budget

Answer: C

NEW QUESTION 6
- (Exam Topic 4)
Which of the following is the GREATEST benefit of having a mature enterprise architecture (EA) in place?

A. Standards-based policies
B. Audit readiness
C. Efficient operations
D. Regulatory compliance

Answer: C

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 4)
WhichT5f the following is the MOST effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage?

A. Enforce sanctions for noncompliance with security procedures.
B. Conduct organization-w>de phishing simulations.
C. Require training on the data handling policy.
D. Require regular testing of the data breach response plan.

Answer: B

NEW QUESTION 10
- (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 10
- (Exam Topic 4)
The MOST important measure of the effectiveness of risk management in project implementation is the percentage of projects:

A. introduced into production without high-risk issues.
B. having the risk register updated regularly.
C. having key risk indicators (KRIs) established to measure risk.
D. having an action plan to remediate overdue issues.

Answer: A

NEW QUESTION 13
- (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 18
- (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 20
- (Exam Topic 4)

Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

A. The program has not decreased threat counts.
B. The program has not considered business impact.
C. The program has been significantly revised
D. The program uses non-customized training modules.

Answer: D

NEW QUESTION 22
- (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 27
- (Exam Topic 4)
A risk practitioner notices a risk scenario associated with data loss at the organization's cloud provider is assigned to the provider Who should the risk scenario be reassigned to?

A. Senior management
B. Chief risk officer (CRO)
C. Vendor manager
D. Data owner

Answer: D

NEW QUESTION 29
- (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 34
- (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 37
- (Exam Topic 4)
Which of the following is PRIMARILY a risk management responsibly of the first line of defense?

A. Implementing risk treatment plans
B. Validating the status of risk mitigation efforts
C. Establishing risk policies and standards
D. Conducting independent reviews of risk assessment results

Answer: C

NEW QUESTION 41
- (Exam Topic 4)
Which of the following should be the FIRST consideration when establishing a new risk governance program?

A. Developing an ongoing awareness and training program
B. Creating policies and standards that are easy to comprehend
C. Embedding risk management into the organization
D. Completing annual risk assessments on critical resources

Answer: B

NEW QUESTION 43
- (Exam Topic 4)
Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

A. Percentage of IT systems recovered within the mean time to restore (MTTR) during the disaster recovery test
B. Percentage of issues arising from the disaster recovery test resolved on time
C. Percentage of IT systems included in the disaster recovery test scope
D. Percentage of IT systems meeting the recovery time objective (RTO) during the disaster recovery test

Answer: D

NEW QUESTION 48
- (Exam Topic 4)
A root because analysis indicates a major service disruption due to a lack of competency of newly hired IT system administrators Who should be accountable for resolving the situation?

A. HR training director
B. Business process owner
C. HR recruitment manager
D. Chief information officer (CIO)

Answer: C

NEW QUESTION 52
- (Exam Topic 4)
If preventive controls cannot be Implemented due to technology limitations, which of the following should be done FIRST to reduce risk7

A. Evaluate alternative controls.
B. Redefine the business process to reduce the risk.
C. Develop a plan to upgrade technology.
D. Define a process for monitoring risk.

Answer: A

NEW QUESTION 57
- (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 61
- (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 64
- (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 69
- (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 72
- (Exam Topic 4)
An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis Which of the following is the MOST important control to ensure the privacy of customer information?

A. Nondisclosure agreements (NDAs)
B. Data anonymization
C. Data cleansing
D. Data encryption

Answer: C

NEW QUESTION 74
- (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 77
- (Exam Topic 4)
When is the BEST to identify risk associated with major project to determine a mitigation plan?

A. Project execution phase
B. Project initiation phase
C. Project closing phase
D. Project planning phase

Answer: D

NEW QUESTION 80
- (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 82
- (Exam Topic 4)
A MAJOR advantage of using key risk indicators (KRis) is that (hey

A. identify when risk exceeds defined thresholds
B. assess risk scenarios that exceed defined thresholds
C. identify scenarios that exceed defined risk appetite
D. help with internal control assessments concerning risk appellate

Answer: B

NEW QUESTION 84
- (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 88
- (Exam Topic 4)
Which of the following is the BEST method to maintain a common view of IT risk within an organization?

A. Collecting data for IT risk assessment

B. Establishing and communicating the IT risk profile
C. Utilizing a balanced scorecard
D. Performing and publishing an IT risk analysis

Answer: C

NEW QUESTION 92
- (Exam Topic 4)
A multinational organization is considering implementing standard background checks to' all new employees A KEY concern regarding this approach

A. fail to identity all relevant issues.
B. be too costly
C. violate laws in other countries
D. be too line consuming

Answer: C

NEW QUESTION 93
- (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 94
- (Exam Topic 3)
Which of The following should be of GREATEST concern for an organization considering the adoption of a bring your own device (BYOD) initiative?

A. Device corruption
B. Data loss
C. Malicious users
D. User support

Answer: B

NEW QUESTION 97
- (Exam Topic 3)
The PRIMARY reason for prioritizing risk scenarios is to:

A. provide an enterprise-wide view of risk
B. support risk response tracking
C. assign risk ownership
D. facilitate risk response decisions.

Answer: D

NEW QUESTION 98
- (Exam Topic 4)
Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?

A. Updating the organizational policy for remote access
B. Creating metrics to track remote connections
C. Implementing multi-factor authentication
D. Updating remote desktop software

Answer: A

NEW QUESTION 100
- (Exam Topic 4)
Which of the following would MOST likely cause management to unknowingly accept excessive risk?

A. Satisfactory audit results
B. Risk tolerance being set too low
C. Inaccurate risk ratings
D. Lack of preventive controls

Answer: C

NEW QUESTION 102
- (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 105
- (Exam Topic 4)
Which of the following BEST enables risk-based decision making in support of a business continuity plan (BCP)?

A. Impact analysis
B. Control analysis
C. Root cause analysis
D. Threat analysis

Answer: A

NEW QUESTION 109
- (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 110
- (Exam Topic 3)
The BEST way to improve a risk register is to ensure the register:

A. is updated based upon significant events.
B. documents possible countermeasures.
C. contains the risk assessment completion date.
D. is regularly audited.

Answer: A

NEW QUESTION 114
- (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 119
- (Exam Topic 3)
Which of the following is the BEST way to determine the potential organizational impact of emerging privacy regulations?

A. Evaluate the security architecture maturity.
B. Map the new requirements to the existing control framework.
C. Charter a privacy steering committee.
D. Conduct a privacy impact assessment (PIA).

Answer: D

NEW QUESTION 122
- (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 126

- (Exam Topic 3)
Winch of the following can be concluded by analyzing the latest vulnerability report for the it infrastructure?

A. Likelihood of a threat
B. Impact of technology risk
C. Impact of operational risk
D. Control weakness

Answer: C

NEW QUESTION 127
- (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 130
- (Exam Topic 3)
Which of the following is MOST important to include in a risk assessment of an emerging technology?

A. Risk response plans
B. Risk and control ownership
C. Key controls
D. Impact and likelihood ratings

Answer: D

NEW QUESTION 132
- (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 136
- (Exam Topic 3)
Which of the following controls are BEST strengthened by a clear organizational code of ethics?

A. Detective controls
B. Administrative controls
C. Technical controls
D. Preventive controls

Answer: B

NEW QUESTION 139
- (Exam Topic 3)
Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

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

Answer: B

NEW QUESTION 142
- (Exam Topic 3)
A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

A. Regulatory requirements may differ in each country.
B. Data sampling may be impacted by various industry restrictions.
C. Business advertising will need to be tailored by country.
D. The data analysis may be ineffective in achieving objectives.

Answer: A

NEW QUESTION 145
- (Exam Topic 3)
Which of the following will help ensure the elective decision-making of an IT risk management committee?

A. Key stakeholders are enrolled as members
B. Approved minutes ate forwarded to senior management
C. Committee meets at least quarterly
D. Functional overlap across the business is minimized

Answer: D

NEW QUESTION 150
- (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 153
- (Exam Topic 3)
The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:

A. the proposed controls are implemented as scheduled.
B. security controls are tested prior to implementation.
C. compliance with corporate policies.
D. the risk response strategy has been decided.

Answer: A

NEW QUESTION 154
- (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 157
- (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 162
- (Exam Topic 3)
Which of the following is the MOST important responsibility of a risk owner?

A. Testing control design
B. Accepting residual risk
C. Establishing business information criteria
D. Establishing the risk register

Answer: C

NEW QUESTION 163
- (Exam Topic 3)
Which of the following should be an element of the risk appetite of an organization?

A. The effectiveness of compensating controls
B. The enterprise's capacity to absorb loss
C. The residual risk affected by preventive controls
D. The amount of inherent risk considered appropriate

Answer:

B

NEW QUESTION 165
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?

A. Percentage of high-risk vulnerabilities missed
B. Number of high-risk vulnerabilities outstanding
C. Defined thresholds for high-risk vulnerabilities
D. Percentage of high-risk vulnerabilities addressed

Answer: D

NEW QUESTION 169
- (Exam Topic 3)
Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

A. Conduct an abbreviated version of the assessment.
B. Report the business unit manager for a possible ethics violation.
C. Perform the assessment as it would normally be done.
D. Recommend an internal auditor perform the review.

Answer: B

NEW QUESTION 172
- (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 175
- (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 177
- (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 181
- (Exam Topic 3)
An IT department originally planned to outsource the hosting of its data center at an overseas location to reduce operational expenses. After a risk assessment, the department has decided to keep the data center in-house. How should the risk treatment response be reflected in the risk register?

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

Answer: A

NEW QUESTION 183
- (Exam Topic 3)
Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

A. Implement controls to bring the risk to a level within appetite and accept the residual risk.
B. Implement a key performance indicator (KPI) to monitor the existing control performance.
C. Accept the residual risk in its entirety and obtain executive management approval.
D. Separate the risk into multiple components and avoid the risk components that cannot be mitigated.

Answer: C

NEW QUESTION 186
- (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 187
- (Exam Topic 3)
The MOST important reason for implementing change control procedures is to ensure:

A. only approved changes are implemented
B. timely evaluation of change events
C. an audit trail exists.
D. that emergency changes are logged.

Answer: A

NEW QUESTION 190
- (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 191
- (Exam Topic 3)
When of the following provides the MOST tenable evidence that a business process control is effective?

A. Demonstration that the control is operating as designed
B. A successful walk-through of the associated risk assessment
C. Management attestation that the control is operating effectively
D. Automated data indicating that risk has been reduced

Answer: C

NEW QUESTION 193
- (Exam Topic 3)
Which of the following represents a vulnerability?

A. An identity thief seeking to acquire personal financial data from an organization
B. Media recognition of an organization's market leadership in its industry
C. A standard procedure for applying software patches two weeks after release
D. An employee recently fired for insubordination

Answer: C

NEW QUESTION 195
- (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 200
- (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 205
- (Exam Topic 3)
An organization discovers significant vulnerabilities in a recently purchased commercial off-the-shelf software product which will not be corrected until the next release. Which of the following is the risk manager's BEST course of action?

A. Review the risk of implementing versus postponing with stakeholders.
B. Run vulnerability testing tools to independently verify the vulnerabilities.
C. Review software license to determine the vendor's responsibility regarding vulnerabilities.
D. Require the vendor to correct significant vulnerabilities prior to installation.

Answer: C

NEW QUESTION 206
- (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 208
- (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 211
- (Exam Topic 3)
Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

A. The sum of residual risk levels for each scenario
B. The loss expectancy for aggregated risk scenarios
C. The highest loss expectancy among the risk scenarios
D. The average of anticipated residual risk levels

Answer: D

NEW QUESTION 213
- (Exam Topic 3)
An internal audit report reveals that not all IT application databases have encryption in place. Which of the following information would be MOST important for assessing the risk impact?

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

Answer: B

NEW QUESTION 217
- (Exam Topic 3)
An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?

A. Number of training sessions completed
B. Percentage of staff members who complete the training with a passing score
C. Percentage of attendees versus total staff
D. Percentage of staff members who attend the training with positive feedback

Answer: B

NEW QUESTION 219
- (Exam Topic 3)
Which of the following BEST indicates whether security awareness training is effective?

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

Answer: B

NEW QUESTION 221
- (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 222
- (Exam Topic 3)
Which of the following would BEST help an enterprise define and communicate its risk appetite?

A. Gap analysis
B. Risk assessment
C. Heat map
D. Risk register

Answer: C

NEW QUESTION 225
- (Exam Topic 3)
Which of the following scenarios represents a threat?

A. Connecting a laptop to a free, open, wireless access point (hotspot)
B. Visitors not signing in as per policy
C. Storing corporate data in unencrypted form on a laptop
D. A virus transmitted on a USB thumb drive

Answer: D

NEW QUESTION 229
- (Exam Topic 3)
During implementation of an intrusion detection system (IDS) to monitor network traffic, a high number of alerts is reported. The risk practitioner should recommend to:

A. reset the alert threshold based on peak traffic
B. analyze the traffic to minimize the false negatives
C. analyze the alerts to minimize the false positives
D. sniff the traffic using a network analyzer

Answer: C

NEW QUESTION 231
- (Exam Topic 3)
The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:

A. inconsistencies between security policies and procedures
B. possible noncompliant activities that lead to data disclosure
C. leading or lagging key risk indicators (KRIs)
D. unknown threats to undermine existing access controls

Answer: B

NEW QUESTION 235
- (Exam Topic 3)
A risk practitioner identifies a database application that has been developed and implemented by the business independently of IT. Which of the following is the BEST course of action?

A. Escalate the concern to senior management.

B. Document the reasons for the exception.
C. Include the application in IT risk assessments.
D. Propose that the application be transferred to IT.

Answer: B

NEW QUESTION 237
- (Exam Topic 3)
Which of the following criteria associated with key risk indicators (KRIs) BEST enables effective risk monitoring?

A. Approval by senior management
B. Low cost of development and maintenance
C. Sensitivity to changes in risk levels
D. Use of industry risk data sources

Answer: C

NEW QUESTION 239
- (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 240
- (Exam Topic 3)
Which of the following BEST enables the identification of trends in risk levels?

A. Correlation between risk levels and key risk indicators (KRIs) is positive.
B. Measurements for key risk indicators (KRIs) are repeatable
C. Quantitative measurements are used for key risk indicators (KRIs).
D. Qualitative definitions for key risk indicators (KRIs) are used.

Answer: B

NEW QUESTION 242
- (Exam Topic 3)
Which of the following will BEST support management reporting on risk?

A. Control self-assessment (CSA)
B. Risk policy requirements
C. A risk register
D. Key performance indicators (KPIs)

Answer: C

NEW QUESTION 243
- (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 248
- (Exam Topic 3)
Which of the following is the MOST critical element to maximize the potential for a successful security implementation?

A. The organization's knowledge
B. Ease of implementation
C. The organization's culture
D. industry-leading security tools

Answer: C

NEW QUESTION 252
- (Exam Topic 3)
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

A. obtain the support of executive management.
B. map the business processes to supporting IT and other corporate resources.
C. identify critical business processes and the degree of reliance on support services.
D. document the disaster recovery process.

Answer: C

NEW QUESTION 254
- (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 258
- (Exam Topic 3)
Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?

A. Ensuring that database changes are correctly applied
B. Enforcing that changes are authorized
C. Deterring illicit actions of database administrators
D. Preventing system developers from accessing production data

Answer: C

NEW QUESTION 260
- (Exam Topic 3)
Which of the following would present the MOST significant risk to an organization when updating the incident response plan?

A. Obsolete response documentation
B. Increased stakeholder turnover
C. Failure to audit third-party providers
D. Undefined assignment of responsibility

Answer: D

NEW QUESTION 262
- (Exam Topic 3)
Winch of the following key control indicators (KCIs) BEST indicates whether security requirements are identified and managed throughout a project He cycle?

A. Number of projects going live without a security review
B. Number of employees completing project-specific security training
C. Number of security projects started in core departments
D. Number of security-related status reports submitted by project managers

Answer: A

NEW QUESTION 264
- (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 269
- (Exam Topic 3)
Which of the following is the BEST way to mitigate the risk to IT infrastructure availability?

A. Establishing a disaster recovery plan (DRP)
B. Establishing recovery time objectives (RTOs)
C. Maintaining a current list of staff contact delays
D. Maintaining a risk register

Answer: D

NEW QUESTION 270
- (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 272
- (Exam Topic 3)
Which of the following should be management's PRIMARY consideration when approving risk response action plans?

A. Ability of the action plans to address multiple risk scenarios
B. Ease of implementing the risk treatment solution
C. Changes in residual risk after implementing the plans
D. Prioritization for implementing the action plans

Answer: C

NEW QUESTION 274
- (Exam Topic 3)
Which of the following is the GREATEST benefit for an organization with a strong risk awareness culture?

A. Reducing the involvement by senior management
B. Using more risk specialists
C. Reducing the need for risk policies and guidelines
D. Discussing and managing risk as a team

Answer: D

NEW QUESTION 278
- (Exam Topic 3)
When reviewing a business continuity plan (BCP). which of the following would be the MOST significant deficiency?

A. BCP testing is net in conjunction with the disaster recovery plan (DRP)
B. Recovery time objectives (RTOs) do not meet business requirements.
C. BCP is often tested using the walk-through method.
D. Each business location has separate, inconsistent BCPs.

Answer: B

NEW QUESTION 283
- (Exam Topic 3)
Which of the following is the MOST important consideration for protecting data assets m a Business application system?

A. Application controls are aligned with data classification lutes
B. Application users are periodically trained on proper data handling practices
C. Encrypted communication is established between applications and data servers
D. Offsite encrypted backups are automatically created by the application

Answer: A

NEW QUESTION 287
- (Exam Topic 3)
Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

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

Answer: B

NEW QUESTION 290
- (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 292
- (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 293
- (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 296
- (Exam Topic 3)
Which of the following is MOST important to the integrity of a security log?

A. Least privilege access
B. Inability to edit
C. Ability to overwrite
D. Encryption

Answer: B

NEW QUESTION 297
- (Exam Topic 3)
Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

A. Key risk indicators (KRIs)
B. Risk scenarios
C. Business impact analysis (BIA)
D. Threat analysis

Answer: B

NEW QUESTION 299
- (Exam Topic 3)
Which of the following is the GREATEST risk associated with the misclassification of data?

A. inadequate resource allocation
B. Data disruption
C. Unauthorized access
D. Inadequate retention schedules

Answer: A

NEW QUESTION 304
- (Exam Topic 3)
Which of the following is a risk practitioner's BEST recommendation to address an organization's need to secure multiple systems with limited IT resources?

A. Apply available security patches.
B. Schedule a penetration test.
C. Conduct a business impact analysis (BIA)
D. Perform a vulnerability analysis.

Answer: C

NEW QUESTION 308
- (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 311
- (Exam Topic 3)
Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

A. Enable data wipe capabilities
B. Penetration testing and session timeouts
C. Implement remote monitoring
D. Enforce strong passwords and data encryption

Answer: D

NEW QUESTION 314
- (Exam Topic 3)
What are the MOST essential attributes of an effective Key control indicator (KCI)?

A. Flexibility and adaptability
B. Measurability and consistency
C. Robustness and resilience
D. Optimal cost and benefit

Answer: B

NEW QUESTION 319
- (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 320
- (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 321
- (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 325
- (Exam Topic 3)
Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

A. Poor access control
B. Unnecessary data storage usage
C. Data inconsistency
D. Unnecessary costs of program changes

Answer: C

NEW QUESTION 329
- (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 332
- (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 333
- (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 337
- (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 342
- (Exam Topic 3)
When formulating a social media policy lo address information leakage, which of the following is the MOST important concern to address?

A. Sharing company information on social media
B. Sharing personal information on social media
C. Using social media to maintain contact with business associates
D. Using social media for personal purposes during working hours

Answer: A

NEW QUESTION 347
- (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 348
- (Exam Topic 3)
Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

A. To enable consistent data on risk to be obtained
B. To allow for proper review of risk tolerance
C. To identify dependencies for reporting risk
D. To provide consistent and clear terminology

Answer: B

NEW QUESTION 352
- (Exam Topic 3)
To communicate the risk associated with IT in business terms, which of the following MUST be defined?

A. Compliance objectives
B. Risk appetite of the organization
C. Organizational objectives

D. Inherent and residual risk

Answer: C

NEW QUESTION 356
- (Exam Topic 3)
The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

A. stakeholder risk tolerance.
B. benchmarking criteria.
C. suppliers used by the organization.
D. the control environment.

Answer: D

NEW QUESTION 357
- (Exam Topic 3)
Which of the following would BEST indicate to senior management that IT processes are improving?

A. Changes in the number of intrusions detected
B. Changes in the number of security exceptions
C. Changes in the position in the maturity model
D. Changes to the structure of the risk register

Answer: B

NEW QUESTION 362
- (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 364
- (Exam Topic 3)
Which of the following should be a risk practitioner's PRIMARY focus when tasked with ensuring organization records are being retained for a sufficient period of time to meet legal obligations?

A. Data duplication processes
B. Data archival processes
C. Data anonymization processes
D. Data protection processes

Answer: B

NEW QUESTION 366
- (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 371
- (Exam Topic 3)
The PRIMARY benefit of using a maturity model is that it helps to evaluate the:

A. capability to implement new processes
B. evolution of process improvements
C. degree of compliance with policies and procedures
D. control requirements.

Answer: B

NEW QUESTION 374
- (Exam Topic 3)
Which of the following is the GREATEST advantage of implementing a risk management program?

A. Enabling risk-aware decisions
B. Promoting a risk-aware culture
C. Improving security governance
D. Reducing residual risk

Answer: A

NEW QUESTION 376
- (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 378
- (Exam Topic 3)
An organization uses a vendor to destroy hard drives. Which of the following would BEST reduce the risk of data leakage?

A. Require the vendor to degauss the hard drives
B. Implement an encryption policy for the hard drives.
C. Require confirmation of destruction from the IT manager.
D. Use an accredited vendor to dispose of the hard drives.

Answer: B

NEW QUESTION 379
- (Exam Topic 3)
Which of the following would be MOST helpful when communicating roles associated with the IT risk management process?

A. Skills matrix
B. Job descriptions
C. RACI chart
D. Organizational chart

Answer: A

NEW QUESTION 383
- (Exam Topic 3)
An organization has outsourced its billing function to an external service provider. Who should own the risk of customer data leakage caused by the service provider?

A. The service provider
B. Vendor risk manager
C. Legal counsel
D. Business process owner

Answer: D

NEW QUESTION 385
- (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 389
- (Exam Topic 3)
Which of the following BEST enforces access control for an organization that uses multiple cloud technologies?

A. Senior management support of cloud adoption strategies
B. Creation of a cloud access risk management policy
C. Adoption of a cloud access security broker (CASB) solution
D. Expansion of security information and event management (SIEM) to cloud services

Answer: C

NEW QUESTION 394

- (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 399
- (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 400
- (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 405
- (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 410
- (Exam Topic 3)
Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?

A. The value at which control effectiveness would fail
B. Thresholds benchmarked to peer organizations
C. A typical operational value
D. A value that represents the intended control state

Answer: A

NEW QUESTION 415
- (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 418
- (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 421
- (Exam Topic 4)
Which of the following is MOST important to ensure when reviewing an organization's risk register?

A. Risk ownership is recorded.
B. Vulnerabilities have separate entries.
C. Control ownership is recorded.
D. Residual risk is less than inherent risk.

Answer: A

NEW QUESTION 425
- (Exam Topic 4)
Which of the following is the MOST important characteristic of a key risk indicator (KRI) to enable decision-making?

A. Monitoring the risk until the exposure is reduced
B. Setting minimum sample sizes to ensure accuracy
C. Listing alternative causes for risk events
D. Illustrating changes in risk trends

Answer: D

NEW QUESTION 427
- (Exam Topic 4)
Senior management is deciding whether to share confidential data with the organization's business partners. The BEST course of action for a risk practitioner would be to submit a report to senior management containing the:

A. possible risk and suggested mitigation plans.
B. design of controls to encrypt the data to be shared.
C. project plan for classification of the data.
D. summary of data protection and privacy legislation.

Answer: A

NEW QUESTION 431
- (Exam Topic 4)
Which of the following BEST balances the costs and benefits of managing IT risk*?

A. Prioritizing and addressing risk in line with risk appetit
B. Eliminating risk through preventive and detective controls
C. Considering risk that can be shared with a third party
D. Evaluating the probability and impact of risk scenarios

Answer: A

NEW QUESTION 436
- (Exam Topic 4)
Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud environment?

A. Reviewing the results of independent audits
B. Performing a site visit to the cloud provider's data center
C. Performing a due diligence review
D. Conducting a risk workshop with key stakeholders

Answer: D

NEW QUESTION 441
- (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 446
- (Exam Topic 4)
A company has recently acquired a customer relationship management (CRM) application from a certified software vendor. Which of the following will BE ST help lo prevent technical vulnerabilities from being exploded?

A. implement code reviews and Quality assurance on a regular basis
B. Verity me software agreement indemnifies the company from losses
C. Review the source coda and error reporting of the application
D. Update the software with the latest patches and updates

Answer: D

NEW QUESTION 448
- (Exam Topic 4)
A risk practitioner recently discovered that personal information from the production environment is required for testing purposes in non-production environments. Which of the following is the BEST recommendation to address this situation?

A. Enable data encryption in the test environment.
B. Prevent the use of production data in the test environment
C. De-identify data before being transferred to the test environment.
D. Enforce multi-factor authentication within the test environment.

Answer: C

NEW QUESTION 451
- (Exam Topic 4)
Reviewing which of the following BEST helps an organization gam insight into its overall risk profile"

A. Risk register
B. Risk appetite
C. Threat landscape
D. Risk metrics

Answer: B

NEW QUESTION 454
- (Exam Topic 4)
Which risk response strategy could management apply to both positive and negative risk that has been identified?

A. Transfer
B. Accept
C. Exploit
D. Mitigate

Answer: B

NEW QUESTION 459
- (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 463
- (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 465
- (Exam Topic 4)
Who should be responsible (of evaluating the residual risk after a compensating control has been

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

Answer: D

NEW QUESTION 470

- (Exam Topic 4)
Which of the following will BEST help to ensure new IT policies address the enterprise's requirements?

A. involve IT leadership in the policy development process
B. Require business users to sign acknowledgment of the poises
C. involve business owners in the pokey development process
D. Provide policy owners with greater enforcement authority

Answer: B

NEW QUESTION 471
- (Exam Topic 4)
Which of the following would BEST facilitate the implementation of data classification requirements?

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

Answer: A

NEW QUESTION 474
- (Exam Topic 4)
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

A. Removing entries from the register after the risk has been treated
B. Recording and tracking the status of risk response plans within the register
C. Communicating the register to key stakeholders
D. Performing regular reviews and updates to the register

Answer: D

NEW QUESTION 475
- (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 479
- (Exam Topic 4)
Which of the following provides the MOST comprehensive information when developing a risk profile for a system?

A. Results of a business impact analysis (BIA)
B. Risk assessment results
C. A mapping of resources to business processes
D. Key performance indicators (KPIs)

Answer: B

NEW QUESTION 484
- (Exam Topic 4)
Which of the following would be a risk practitioner’s BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

A. Perform a gap analysis
B. Conduct system testing
C. Implement compensating controls
D. Update security policies

Answer: A

NEW QUESTION 485
- (Exam Topic 4)
When performing a risk assessment of a new service to support a core business process, which of the following should be done FIRST to ensure continuity of operations?

A. Define metrics for restoring availability.
B. Identify conditions that may cause disruptions.
C. Review incident response procedures.
D. Evaluate the probability of risk events.

Answer: B

NEW QUESTION 488
- (Exam Topic 4)
Which of the following potential scenarios associated with the implementation of a new database technology presents the GREATEST risk to an organization?

A. The organization may not have a sufficient number of skilled resources.
B. Application and data migration cost for backups may exceed budget.
C. Data may not be recoverable due to system failures.
D. The database system may not be scalable in the future.

Answer: B

NEW QUESTION 491
- (Exam Topic 4)
Which of the following is the PRIMARY reason for sharing risk assessment reports with senior stakeholders?

A. To support decision-making for risk response
B. To hold risk owners accountable for risk action plans
C. To secure resourcing for risk treatment efforts
D. To enable senior management to compile a risk profile

Answer: A

NEW QUESTION 495
- (Exam Topic 4)
During an acquisition, which of the following would provide the MOST useful input to the parent company's risk practitioner when developing risk scenarios for the post-acquisition phase?

A. Risk management framework adopted by each company
B. Risk registers of both companies
C. IT balanced scorecard of each company
D. Most recent internal audit findings from both companies

Answer: C

NEW QUESTION 499
- (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 501
- (Exam Topic 4)
Which of the following will BEST help to ensure key risk indicators (KRIs) provide value to risk owners?

A. Ongoing training
B. Timely notification
C. Return on investment (ROI)
D. Cost minimization

Answer: B

NEW QUESTION 502
- (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 504
- (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 508
- (Exam Topic 4)
As pan of business continuity planning, which of the following is MOST important to include m a business impact analysis (BlA)?

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 510
- (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 511
- (Exam Topic 4)
Which of the following is the MOST important reason to validate that risk responses have been executed as outlined in the risk response plan''

A. To ensure completion of the risk assessment cycle
B. To ensure controls arc operating effectively
C. To ensure residual risk Is at an acceptable level
D. To ensure control costs do not exceed benefits

Answer: A

NEW QUESTION 513
- (Exam Topic 4)
Which of the following is the result of a realized risk scenario?

A. Technical event
B. Threat event
C. Vulnerability event
D. Loss event

Answer: D

NEW QUESTION 518
- (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 519
- (Exam Topic 4)
A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner s NEXT step? r

A. Prepare a business case for the response options.
B. Identify resources for implementing responses.
C. Develop a mechanism for monitoring residual risk.
D. Update the risk register with the results.

Answer: D

NEW QUESTION 524
- (Exam Topic 4)
Which stakeholder is MOST important to include when defining a risk profile during me selection process for a new third party application'?

A. The third-party risk manager
B. The application vendor

C. The business process owner
D. The information security manager

Answer: B

NEW QUESTION 525
- (Exam Topic 4)
An organization has operations in a location that regularly experiences severe weather events. Which of the following would BEST help to mitigate the risk to operations?

A. Prepare a cost-benefit analysis to evaluate relocation.
B. Prepare a disaster recovery plan (DRP).
C. Conduct a business impact analysis (BIA) for an alternate location.
D. Develop a business continuity plan (BCP).

Answer: D

NEW QUESTION 530
- (Exam Topic 4)
Which of the following is the MAIN purpose of monitoring risk?

A. Communication
B. Risk analysis
C. Decision support
D. Benchmarking

Answer: A

NEW QUESTION 532
- (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 537
- (Exam Topic 4)
Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

A. Accountability may not be clearly defined.
B. Risk ratings may be inconsistently applied.
C. Different risk taxonomies may be used.
D. Mitigation efforts may be duplicated.

Answer: A

NEW QUESTION 538
- (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 543
- (Exam Topic 4)
Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

A. Service level agreements (SLAs) have not been met over the last quarter.
B. The service contract is up for renewal in less than thirty days.
C. Key third-party personnel have recently been replaced.
D. Monthly service charges are significantly higher than industry norms.

Answer: C

NEW QUESTION 544
- (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 548
- (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 550
- (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 552
- (Exam Topic 4)
When documenting a risk response, which of the following provides the STRONGEST evidence to support the decision?

A. Verbal majority acceptance of risk by committee
B. List of compensating controls
C. IT audit follow-up responses
D. A memo indicating risk acceptance

Answer: C

NEW QUESTION 556
- (Exam Topic 4)
An organization recently configured a new business division Which of the following is MOST likely to be affected?

A. Risk profile
B. Risk culture
C. Risk appetite
D. Risk tolerance

Answer: A

NEW QUESTION 561
- (Exam Topic 4)
Which of the following is the BEST recommendation to address recent IT risk trends that indicate social engineering attempts are increasing in the organization?

A. Conduct a simulated phishing attack.
B. Update spam filters
C. Revise the acceptable use policy
D. Strengthen disciplinary procedures

Answer: A

NEW QUESTION 562
- (Exam Topic 4)
Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

A. Increase in mitigating control costs
B. Increase in risk event impact
C. Increase in risk event likelihood
D. Increase in cybersecurity premium

Answer: C

NEW QUESTION 565
- (Exam Topic 4)
Which of the following BEST facilitates the identification of appropriate key performance indicators (KPIs) for a risk management program?

A. Reviewing control objectives
B. Aligning with industry best practices
C. Consulting risk owners
D. Evaluating KPIs in accordance with risk appetite

Answer: C

NEW QUESTION 567
- (Exam Topic 4)
Which of the following s MOST likely to deter an employee from engaging in inappropriate use of company owned IT systems?

A. A centralized computer security response team
B. Regular performance reviews and management check-ins
C. Code of ethics training for all employees
D. Communication of employee activity monitoring

Answer: D

NEW QUESTION 570
- (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 572
- (Exam Topic 4)
Which of the following is the MOST important consideration when communicating the risk associated with technology end-of-life to business owners?

A. Cost and benefit
B. Security and availability
C. Maintainability and reliability
D. Performance and productivity

Answer: A

NEW QUESTION 573
- (Exam Topic 4)
A control process has been implemented in response to a new regulatory requirement, but has significantly reduced productivity. Which of the following is the BEST way to resolve this concern?

A. Absorb the loss in productivity.
B. Request a waiver to the requirements.
C. Escalate the issue to senior management
D. Remove the control to accommodate business objectives.

Answer: C

NEW QUESTION 575
- (Exam Topic 4)
Which of the following should be considered FIRST when creating a comprehensive IT risk register?

A. Risk management budget
B. Risk mitigation policies
C. Risk appetite
D. Risk analysis techniques

Answer: C

NEW QUESTION 576
- (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 580
- (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 581
- (Exam Topic 4)
Which of the following is MOST important to promoting a risk-aware culture?

A. Regular testing of risk controls
B. Communication of audit findings
C. Procedures for security monitoring
D. Open communication of risk reporting

Answer: D

NEW QUESTION 583
- (Exam Topic 4)
The MAJOR reason to classify information assets is

A. maintain a current inventory and catalog of information assets
B. determine their sensitivity and critical
C. establish recovery time objectives (RTOs)
D. categorize data into groups

Answer: C

NEW QUESTION 585
- (Exam Topic 4)
Which of the following is the PRIMARY objective of maintaining an information asset inventory?

A. To provide input to business impact analyses (BIAs)
B. To protect information assets
C. To facilitate risk assessments
D. To manage information asset licensing

Answer: B

NEW QUESTION 588
- (Exam Topic 4)
In order to efficiently execute a risk response action plan, it is MOST important for the emergency response team members to understand:

A. system architecture in target areas.
B. IT management policies and procedures.
C. business objectives of the organization.
D. defined roles and responsibilities.

Answer: D

NEW QUESTION 590
- (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 594
- (Exam Topic 4)
Which of the following is the BEST way to determine whether system settings are in alignment with control baselines?

A. Configuration validation
B. Control attestation
C. Penetration testing

D. Internal audit review

Answer: A

NEW QUESTION 595
- (Exam Topic 4)
When creating a separate IT risk register for a large organization, which of the following is MOST important to consider with regard to the existing corporate risk 'register?

A. Leveraging business risk professionals
B. Relying on generic IT risk scenarios
C. Describing IT risk in business terms
D. Using a common risk taxonomy

Answer: D

NEW QUESTION 598
- (Exam Topic 4)
Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

A. Ability to determine business impact
B. Up-to-date knowledge on risk responses
C. Decision-making authority for risk treatment
D. Awareness of emerging business threats

Answer: A

NEW QUESTION 599
- (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 604
- (Exam Topic 4)
Which of the following would be the BEST way for a risk practitioner to validate the effectiveness of a patching program?

A. Conduct penetration testing.
B. Interview IT operations personnel.
C. Conduct vulnerability scans.
D. Review change control board documentation.

Answer: C

NEW QUESTION 607
- (Exam Topic 4)
Effective risk communication BEST benefits an organization by:

A. helping personnel make better-informed decisions
B. assisting the development of a risk register.
C. improving the effectiveness of IT controls.
D. increasing participation in the risk assessment process.

Answer: A

NEW QUESTION 609
- (Exam Topic 4)
Before assigning sensitivity levels to information it is MOST important to:

A. define recovery time objectives (RTOs).
B. define the information classification policy
C. conduct a sensitivity analyse
D. Identify information custodians

Answer: B

NEW QUESTION 611
- (Exam Topic 4)
Which of the following is MOST useful for measuring the existing risk management process against a desired state?

A. Balanced scorecard
B. Risk management framework
C. Capability maturity model
D. Risk scenario analysis

Answer: C

NEW QUESTION 613
- (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 614
- (Exam Topic 4)
Which of the following is MOST important for senior management to review during an acquisition?

A. Risk appetite and tolerance
B. Risk framework and methodology
C. Key risk indicator (KRI) thresholds
D. Risk communication plan

Answer: A

NEW QUESTION 618
- (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 622
- (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 627
- (Exam Topic 4)
What is the BEST recommendation to reduce the risk associated with potential system compromise when a vendor stops releasing security patches and updates for a business-critical legacy system?

A. Segment the system on its own network.
B. Ensure regular backups take place.
C. Virtualize the system in the cloud.
D. Install antivirus software on the system.

Answer: A

NEW QUESTION 629
- (Exam Topic 4)
Which of the following is the MOST important step to ensure regulatory requirements are adequately addressed within an organization?

A. Obtain necessary resources to address regulatory requirements
B. Develop a policy framework that addresses regulatory requirements
C. Perform a gap analysis against regulatory requirements.
D. Employ IT solutions that meet regulatory requirements.

Answer: B

NEW QUESTION 632

- (Exam Topic 4)
Which of the following should be accountable for ensuring that media containing financial information are adequately destroyed per an organization's data disposal policy?

A. Compliance manager
B. Data architect
C. Data owner
D. Chief information officer (CIO)

Answer: C

NEW QUESTION 636
- (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 637
- (Exam Topic 4)
An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:

A. a recognized industry control framework
B. guidance provided by the external auditor
C. the service provider's existing controls
D. The organization's specific control requirements

Answer: D

NEW QUESTION 638
- (Exam Topic 4)
An IT risk threat analysis is BEST used to establish

A. risk scenarios
B. risk maps
C. risk appetite
D. risk ownership.

Answer: A

NEW QUESTION 641
- (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 643
- (Exam Topic 4)
After the implementation of internal of Things (IoT) devices, new risk scenarios were identified. What is the PRIMARY reason to report this information to risk owners?

A. To reevaluate continued use to IoT devices
B. The add new controls to mitigate the risk
C. The recommend changes to the IoT policy
D. To confirm the impact to the risk profile

Answer: D

NEW QUESTION 646
- (Exam Topic 4)
An organization is implementing robotic process automation (RPA) to streamline business processes. Given that implementation of this technology is expected to impact existing controls, which of the following is the risk practitioner's BEST course of action?

A. Reassess whether mitigating controls address the known risk in the processes.
B. Update processes to address the new technology.
C. Update the data governance policy to address the new technology.
D. Perform a gap analysis of the impacted processes.

Answer: A

NEW QUESTION 647
- (Exam Topic 4)
Which of the following is MOST important to determine as a result of a risk assessment?

A. Process ownership
B. Risk appetite statement
C. Risk tolerance levels
D. Risk response options

Answer: D

NEW QUESTION 652
- (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 655
- (Exam Topic 4)
The MAIN purpose of selecting a risk response is to.

A. ensure compliance with local regulatory requirements
B. demonstrate the effectiveness of risk management practices.
C. ensure organizational awareness of the risk level
D. mitigate the residual risk to be within tolerance

Answer: C

NEW QUESTION 656
- (Exam Topic 4)
What should be the PRIMARY consideration related to data privacy protection when there are plans for a business initiative to make use of personal information?

A. Do not collect or retain data that is not needed.
B. Redact data where possible.
C. Limit access to the personal data.
D. Ensure all data is encrypted at rest and during transit.

Answer: D

NEW QUESTION 659
- (Exam Topic 4)
Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

A. Some critical business applications are not included in the plan
B. Several recovery activities will be outsourced
C. The plan is not based on an internationally recognized framework
D. The chief information security officer (CISO) has not approved the plan

Answer: A

NEW QUESTION 660
- (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 663
- (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 667
- (Exam Topic 4)
An organization recently implemented a machine learning-based solution to monitor IT usage and analyze user behavior in an effort to detect internal fraud. Which of the following is MOST likely to be reassessed as a result of this initiative?

A. Risk likelihood
B. Risk culture
C. Risk appetite
D. Risk capacity

Answer: A

NEW QUESTION 671
- (Exam Topic 4)
After entering a large number of low-risk scenarios into the risk register, it is MOST important for the risk practitioner to:

A. prepare a follow-up risk assessment.
B. recommend acceptance of the risk scenarios.
C. reconfirm risk tolerance levels.
D. analyze changes to aggregate risk.

Answer: D

NEW QUESTION 672
- (Exam Topic 4)
The BEST key performance indicator (KPI) to measure the effectiveness of the security patching process is the percentage of patches installed:

A. by the security administration team.
B. successfully within the expected time frame.
C. successfully during the first attempt.
D. without causing an unplanned system outage.

Answer: B

NEW QUESTION 676
- (Exam Topic 4)
Which of the following should be the PRIMARY basis for prioritizing risk responses?

A. The impact of the risk
B. The replacement cost of the business asset
C. The cost of risk mitigation controls
D. The classification of the business asset

Answer: A

NEW QUESTION 681
- (Exam Topic 4)
Which of the following is MOST important when determining risk appetite?

A. Assessing regulatory requirements
B. Benchmarking against industry standards
C. Gaining management consensus
D. Identifying risk tolerance

Answer: C

NEW QUESTION 684
- (Exam Topic 4)
Which of the following is MOST important for an organization to consider when developing its IT strategy?

A. IT goals and objectives
B. Organizational goals and objectives
C. The organization's risk appetite statement
D. Legal and regulatory requirements

Answer: C

NEW QUESTION 686
- (Exam Topic 4)
Which of the following is a risk practitioner's BEST course of action after identifying risk scenarios related to noncompliance with new industry regulations?

A. Escalate to senior management.
B. Transfer the risk.
C. Implement monitoring controls.
D. Recalculate the risk.

Answer: D

NEW QUESTION 689
- (Exam Topic 3)
A risk practitioner has discovered a deficiency in a critical system that cannot be patched. Which of the following should be the risk practitioner's FIRST course of action?

A. Report the issue to internal audit.
B. Submit a request to change management.
C. Conduct a risk assessment.
D. Review the business impact assessment.

Answer: C

NEW QUESTION 694
- (Exam Topic 3)
Upon learning that the number of failed back-up attempts continually exceeds the current risk threshold, the risk practitioner should:

A. inquire about the status of any planned corrective actions
B. keep monitoring the situation as there is evidence that this is normal
C. adjust the risk threshold to better reflect actual performance
D. initiate corrective action to address the known deficiency

Answer: D

NEW QUESTION 695
- (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 698
- (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 703
- (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 705
- (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 710

- (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 714
- (Exam Topic 3)
Who should be PRIMARILY responsible for establishing an organization's IT risk culture?

A. Business process owner
B. Executive management
C. Risk management
D. IT management

Answer: B

NEW QUESTION 719
- (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 724
- (Exam Topic 3)
An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

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

Answer: D

NEW QUESTION 726
- (Exam Topic 3)
An organization's risk register contains a large volume of risk scenarios that senior management considers overwhelming. Which of the following would BEST help to improve the risk register?

A. Analyzing the residual risk components
B. Performing risk prioritization
C. Validating the risk appetite level
D. Conducting a risk assessment

Answer: D

NEW QUESTION 730
- (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 733
- (Exam Topic 3)
Which of the following BEST assists in justifying an investment in automated controls?

A. Cost-benefit analysis
B. Alignment of investment with risk appetite
C. Elimination of compensating controls
D. Reduction in personnel costs

Answer: A

NEW QUESTION 735
- (Exam Topic 3)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 740
- (Exam Topic 3)
The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

A. availability of fault tolerant software.
B. strategic plan for business growth.
C. vulnerability scan results of critical systems.
D. redundancy of technical infrastructure.

Answer: D

NEW QUESTION 744
- (Exam Topic 3)
Which of the following is the FIRST step in risk assessment?

A. Review risk governance
B. Asset identification
C. Identify risk factors
D. Inherent risk identification

Answer: B

NEW QUESTION 745
- (Exam Topic 3)
A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

A. Monitor processes to ensure recent updates are being followed.
B. Communicate to those who test and promote changes.
C. Conduct a cost-benefit analysis to justify the cost of the control.
D. Assess the maturity of the change management process.

Answer: A

NEW QUESTION 746
- (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 750
- (Exam Topic 3)
The PRIMARY purpose of IT control status reporting is to:

A. ensure compliance with IT governance strategy.
B. assist internal audit in evaluating and initiating remediation efforts.
C. benchmark IT controls with Industry standards.
D. facilitate the comparison of the current and desired states.

Answer: A

NEW QUESTION 752
- (Exam Topic 3)
The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

A. resources to monitor backups
B. restoration monitoring reports
C. backup recovery requests

D. recurring restore failures

Answer: D

NEW QUESTION 754
- (Exam Topic 3)
Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

A. Occurrences of specific events
B. A performance measurement
C. The risk tolerance level
D. Risk scenarios

Answer: C

NEW QUESTION 756
- (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 759
- (Exam Topic 3)
Which of the following poses the GREATEST risk to an organization's operations during a major it transformation?

A. Lack of robust awareness programs
B. infrequent risk assessments of key controls
C. Rapid changes in IT procedures
D. Unavailability of critical IT systems

Answer: D

NEW QUESTION 761
- (Exam Topic 3)
The acceptance of control costs that exceed risk exposure MOST likely demonstrates:

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

Answer: C

NEW QUESTION 765
- (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 769
- (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 772
- (Exam Topic 3)
Which of the following should a risk practitioner recommend FIRST when an increasing trend of risk events and subsequent losses has been identified?

A. Conduct root cause analyses for risk events.

B. Educate personnel on risk mitigation strategies.
C. Integrate the risk event and incident management processes.
D. Implement controls to prevent future risk events.

Answer: C

NEW QUESTION 776
- (Exam Topic 3)
The MAIN purpose of reviewing a control after implementation is to validate that the control:

A. operates as intended.
B. is being monitored.
C. meets regulatory requirements.
D. operates efficiently.

Answer: A

NEW QUESTION 780
- (Exam Topic 3)
Which of the following BEST indicates the efficiency of a process for granting access privileges?

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

Answer: C

NEW QUESTION 784
- (Exam Topic 3)
A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

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

Answer: A

NEW QUESTION 787
- (Exam Topic 3)
A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

A. Monitor the databases for abnormal activity
B. Approve exception to allow the software to continue operating
C. Require the software vendor to remediate the vulnerabilities
D. Accept the risk and let the vendor run the software as is

Answer: C

NEW QUESTION 792
- (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 793
- (Exam Topic 3)
Which of the following approaches would BEST help to identify relevant risk scenarios?

A. Engage line management in risk assessment workshops.
B. Escalate the situation to risk leadership.
C. Engage internal audit for risk assessment workshops.
D. Review system and process documentation.

Answer: A

NEW QUESTION 794

- (Exam Topic 3)
Which of the following would provide the MOST useful information to a risk owner when reviewing the progress of risk mitigation?

A. Key audit findings
B. Treatment plan status
C. Performance indicators
D. Risk scenario results

Answer: C

NEW QUESTION 799
- (Exam Topic 3)
Which of the following should be done FIRST when information is no longer required to support business objectives?

A. Archive the information to a backup database.
B. Protect the information according to the classification policy.
C. Assess the information against the retention policy.
D. Securely and permanently erase the information

Answer: C

NEW QUESTION 803
- (Exam Topic 3)
Which of the following is the MOST common concern associated with outsourcing to a service provider?

A. Lack of technical expertise
B. Combining incompatible duties
C. Unauthorized data usage
D. Denial of service attacks

Answer: C

NEW QUESTION 808
- (Exam Topic 3)
In an organization that allows employee use of social media accounts for work purposes, which of the following is the BEST way to protect company sensitive information from being exposed?

A. Educating employees on what needs to be kept confidential
B. Implementing a data loss prevention (DLP) solution
C. Taking punitive action against employees who expose confidential data
D. Requiring employees to sign nondisclosure agreements

Answer: B

NEW QUESTION 812
- (Exam Topic 3)
Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?

A. Unknown vulnerabilities
B. Legacy technology systems
C. Network isolation
D. Overlapping threats

Answer: D

NEW QUESTION 817
- (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 819
- (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 821
- (Exam Topic 3)
During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?

A. Conduct a comprehensive review of access management processes.
B. Declare a security incident and engage the incident response team.
C. Conduct a comprehensive awareness session for system administrators.
D. Evaluate system administrators' technical skills to identify if training is required.

Answer: A

NEW QUESTION 826
- (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 831
- (Exam Topic 3)
An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

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

Answer: B

NEW QUESTION 832
- (Exam Topic 3)
An IT control gap has been identified in a key process. Who would be the MOST appropriate owner of the risk associated with this gap?

A. Key control owner
B. Operational risk manager
C. Business process owner
D. Chief information security officer (CISO)

Answer: A

NEW QUESTION 834
- (Exam Topic 3)
Which of the following would be a risk practitioner'$ BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

A. Manage cyber risk according to the organization's risk management framework.
B. Define cyber roles and responsibilities across the organization
C. Conduct cyber risk awareness training tailored specifically for senior management
D. Implement a cyber risk program based on industry best practices

Answer: B

NEW QUESTION 839
- (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 843
- (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 848
- (Exam Topic 3)
Which of the following should be the MOST important consideration when performing a vendor risk assessment?

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

Answer: B

NEW QUESTION 850
- (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 852
- (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 853
- (Exam Topic 3)
Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (AI) solutions into the organization?

A. AI requires entirely new risk management processes.
B. AI potentially introduces new types of risk.
C. AI will result in changes to business processes.
D. Third-party AI solutions increase regulatory obligations.

Answer: B

NEW QUESTION 856
- (Exam Topic 3)
An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

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

Answer: C

NEW QUESTION 861
- (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 862
- (Exam Topic 2)
Which of the following is MOST important for an organization that wants to reduce IT operational risk?

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

Answer: C

NEW QUESTION 865
- (Exam Topic 2)
Which of the following risk scenarios would be the GREATEST concern as a result of a single sign-on implementation?

A. User access may be restricted by additional security.
B. Unauthorized access may be gained to multiple systems.
C. Security administration may become more complex.
D. User privilege changes may not be recorded.

Answer: B

NEW QUESTION 868
- (Exam Topic 2)
A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner's FIRST course of action?

A. Update the KRI threshold.
B. Recommend additional controls.
C. Review incident handling procedures.
D. Perform a root cause analysis.

Answer: D

NEW QUESTION 869
- (Exam Topic 2)
Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?

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

Answer: A

NEW QUESTION 870
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of a control action plan's implementation?

A. Increased number of controls
B. Reduced risk level
C. Increased risk appetite
D. Stakeholder commitment

Answer: B

NEW QUESTION 873
- (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 876
- (Exam Topic 2)
The purpose of requiring source code escrow in a contractual agreement is to:

A. ensure that the source code is valid and exists.
B. ensure that the source code is available if the vendor ceases to exist.
C. review the source code for adequacy of controls.
D. ensure the source code is available when bugs occur.

Answer: B

NEW QUESTION 881

- (Exam Topic 2)
Mapping open risk issues to an enterprise risk heat map BEST facilitates:

A. risk response.
B. control monitoring.
C. risk identification.
D. risk ownership.

Answer: A

NEW QUESTION 886
- (Exam Topic 2)
When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:

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

Answer: B

NEW QUESTION 890
- (Exam Topic 2)
Which of the following BEST measures the efficiency of an incident response process?

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

Answer: C

NEW QUESTION 892
- (Exam Topic 2)
An organization is making significant changes to an application. At what point should the application risk profile be updated?

A. After user acceptance testing (UAT)
B. Upon release to production
C. During backlog scheduling
D. When reviewing functional requirements

Answer: D

NEW QUESTION 894
- (Exam Topic 2)
IT disaster recovery point objectives (RPOs) should be based on the:

A. maximum tolerable downtime.
B. maximum tolerable loss of data.
C. need of each business unit.
D. type of business.

Answer: C

NEW QUESTION 898
- (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 903
- (Exam Topic 2)
A risk practitioner has just learned about new done FIRST?

A. Notify executive management.
B. Analyze the impact to the organization.
C. Update the IT risk register.
D. Design IT risk mitigation plans.

Answer: B

NEW QUESTION 907
- (Exam Topic 2)
Which of the following is MOST commonly compared against the risk appetite?

A. IT risk
B. Inherent risk
C. Financial risk
D. Residual risk

Answer: D

NEW QUESTION 910
- (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 915
- (Exam Topic 2)
Which of the following is the MOST important consideration when selecting either a qualitative or quantitative risk analysis?

A. Expertise in both methodologies
B. Maturity of the risk management program
C. Time available for risk analysis
D. Resources available for data analysis

Answer: D

NEW QUESTION 919
- (Exam Topic 2)
When reporting risk assessment results to senior management, which of the following is MOST important to include to enable risk-based decision making?

A. Risk action plans and associated owners
B. Recent audit and self-assessment results
C. Potential losses compared to treatment cost
D. A list of assets exposed to the highest risk

Answer: A

NEW QUESTION 920
- (Exam Topic 2)
A risk practitioner shares the results of a vulnerability assessment for a critical business application with the business manager. Which of the following is the NEXT step?

A. Develop a risk action plan to address the findings.
B. Evaluate the impact of the vulnerabilities to the business application.
C. Escalate the findings to senior management and internal audit.
D. Conduct a penetration test to validate the vulnerabilities from the findings.

Answer: B

NEW QUESTION 923
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CRISC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CRISC Product From:

https://www.2passeasy.com/dumps/CRISC/

Money Back Guarantee

CRISC Practice Exam Features:

* CRISC Questions and Answers Updated Frequently

* CRISC Practice Questions Verified by Expert Senior Certified Staff

* CRISC Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CRISC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year