Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (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 2
- (Exam Topic 3)
The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.

Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading to data compromise	Risk Council	End-User Computing Manager AND Inventory Manager	IT Operations Manager AND Security Operations	Low Likelihood	Very Serious	0.120	Mitigate	Purchase and acquire data encryption software for mobile
R003	Fire Hazard	A fire accident may destroy data center equipment and servers leading to loss of availability and services	Information Security Department	Data Center Facilities Manager	Facilities Manager	Low Likelihood	Serious	0.060	Transfer	Buy fire hazard insurance policy
		A disgruntled								

Significant	0.10	Low Likelihood	0.30
Serious	0.20	Likely	0.50
Very Serious	0.40	Highly Likely	0.70
Catastrophic	0.80	Near Certainty	0.90

After implementing countermeasures listed in ''Risk Response Descriptions'' for each of the Risk IDs, which of the following component of the register MUST change?

A. Risk Impact Rating
B. Risk Owner
C. Risk Likelihood Rating
D. Risk Exposure

Answer: B

NEW QUESTION 3
- (Exam Topic 3)
Which of the following BEST supports ethical IT risk management practices?

A. Robust organizational communication channels
B. Mapping of key risk indicators (KRIs) to corporate strategy
C. Capability maturity models integrated with risk management frameworks
D. Rigorously enforced operational service level agreements (SLAs)

Answer: A

NEW QUESTION 4
- (Exam Topic 3)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery test of critical business processes?

A. Percentage of job failures identified and resolved during the recovery process
B. Percentage of processes recovered within the recovery time and point objectives
C. Number of current test plans and procedures
D. Number of issues and action items resolved during the recovery test

Answer: B

NEW QUESTION 5
- (Exam Topic 3)
Which of the following is the BEST reason to use qualitative measures to express residual risk levels related to emerging threats?

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

Answer: C

NEW QUESTION 6
- (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 7
- (Exam Topic 3)
When updating the risk register after a risk assessment, which of the following is MOST important to include?

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

Answer: C

NEW QUESTION 8
- (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 9
- (Exam Topic 3)
Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?

A. Analyzing cyber intelligence reports
B. Engaging independent cybersecurity consultants
C. Increasing the frequency of updates to the risk register
D. Reviewing the outcome of the latest security risk assessment

Answer: D

NEW QUESTION 10
- (Exam Topic 3)
Several network user accounts were recently created without the required management approvals. Which of the following would be the risk practitioner's BEST recommendation to address this situation?

A. Conduct a comprehensive compliance review.
B. Develop incident response procedures for noncompliance.
C. Investigate the root cause of noncompliance.
D. Declare a security breach and Inform management.

Answer: C

NEW QUESTION 10
- (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 12
- (Exam Topic 3)
Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?

A. Key risk indicators (KRIs)
B. Key management indicators (KMIs)
C. Key performance indicators (KPIs)
D. Key control indicators (KCIs)

Answer: D

NEW QUESTION 17
- (Exam Topic 3)
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 21
- (Exam Topic 3)
Which of the following is the BEST indicator of an effective IT security awareness program?

A. Decreased success rate of internal phishing tests
B. Decreased number of reported security incidents
C. Number of disciplinary actions issued for security violations
D. Number of employees that complete security training

Answer: A

NEW QUESTION 23
- (Exam Topic 3)
Which of the following would MOST likely cause a risk practitioner to change the likelihood rating in the risk register?

A. Risk appetite
B. Control cost
C. Control effectiveness
D. Risk tolerance

Answer: C

NEW QUESTION 26
- (Exam Topic 3)
The MAIN reason for creating and maintaining a risk register is to:

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

Answer: D

NEW QUESTION 29
- (Exam Topic 3)
An organization moved its payroll system to a Software as a Service (SaaS) application. A new data privacy regulation stipulates that data can only be processed within the country where it is collected. Which of the following should be done FIRST when addressing this situation?

A. Analyze data protection methods.
B. Understand data flows.
C. Include a right-to-audit clause.
D. Implement strong access controls.

Answer: B

NEW QUESTION 31
- (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 35
- (Exam Topic 3)
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

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

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

Answer: A

NEW QUESTION 40
- (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 43
- (Exam Topic 3)
An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?

A. Conduct a risk analysis.
B. Initiate a remote data wipe.
C. Invoke the incident response plan
D. Disable the user account.

Answer: C

NEW QUESTION 45
- (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 46
- (Exam Topic 3)
Which of the following would MOST effectively reduce risk associated with an increase of online transactions on a retailer website?

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

Answer: C

NEW QUESTION 47
- (Exam Topic 3)
Which of the following is the MOST effective way to integrate risk and compliance management?

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

Answer: A

NEW QUESTION 50
- (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 52
- (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 56
- (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 57
- (Exam Topic 3)
Which of the following is the PRIMARY reason to use key control indicators (KCIs) to evaluate control operating effectiveness?

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

Answer: C

NEW QUESTION 61
- (Exam Topic 3)
The PRIMARY purpose of using a framework for risk analysis is to:

A. improve accountability
B. improve consistency
C. help define risk tolerance
D. help develop risk scenarios.

Answer: C

NEW QUESTION 65
- (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 69
- (Exam Topic 3)
A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

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

Answer: D

NEW QUESTION 70
- (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 74
- (Exam Topic 3)
Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

A. Align business objectives with risk appetite.
B. Enable risk-based decision making.
C. Design and implement risk response action plans.
D. Update risk responses in the risk register

Answer: B

NEW QUESTION 77
- (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 80
- (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 85
- (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 86
- (Exam Topic 3)
The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

A. data logging and monitoring
B. data mining and analytics

C. data classification and labeling
D. data retention and destruction

Answer: C

NEW QUESTION 88
- (Exam Topic 3)
To help identify high-risk situations, an organization should:

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

Answer: A

NEW QUESTION 91
- (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 95
- (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 98
- (Exam Topic 3)
While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

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

Answer: B

NEW QUESTION 99
- (Exam Topic 3)
A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?

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

Answer: B

NEW QUESTION 101
- (Exam Topic 3)
An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

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

Answer: C

NEW QUESTION 104

- (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 108
- (Exam Topic 3)
A maturity model is MOST useful to an organization when it:

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

Answer: C

NEW QUESTION 113
- (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 114
- (Exam Topic 3)
Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?

A. Data encryption has not been applied to all sensitive data across the organization.
B. There are many data assets across the organization that need to be classified.
C. Changes to information handling procedures are not documented.
D. Changes to data sensitivity during the data life cycle have not been considered.

Answer: D

NEW QUESTION 118
- (Exam Topic 3)
When reviewing the business continuity plan (BCP) of an online sales order system, a risk practitioner notices that the recovery time objective (RTO) has a shorter lime than what is defined in the disaster recovery plan (DRP). Which of the following is the BEST way for the risk practitioner to address this concern?

A. Adopt the RTO defined in the BCR
B. Update the risk register to reflect the discrepancy.
C. Adopt the RTO defined in the DRP.
D. Communicate the discrepancy to the DR manager for follow-up.

Answer: D

NEW QUESTION 120
- (Exam Topic 3)
Which of the following should be implemented to BEST mitigate the risk associated with infrastructure updates?

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

Answer: C

NEW QUESTION 124
- (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 128
- (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 130
- (Exam Topic 3)
An organization has initiated a project to launch an IT-based service to customers and take advantage of being the first to market. Which of the following should be of GREATEST concern to senior management?

A. More time has been allotted for testing.
B. The project is likely to deliver the product late.
C. A new project manager is handling the project.
D. The cost of the project will exceed the allotted budget.

Answer: B

NEW QUESTION 135
- (Exam Topic 3)
Which of the following is the BEST Key control indicator KCO to monitor the effectiveness of patch management?

A. Percentage of legacy servers out of support
B. Percentage of severs receiving automata patches
C. Number of unremediated vulnerabilities
D. Number of intrusion attempts

Answer: D

NEW QUESTION 139
- (Exam Topic 3)
Which of the following is the PRIMARY role of a data custodian in the risk management process?

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

Answer: D

NEW QUESTION 143
- (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 145
- (Exam Topic 3)
The PRIMARY advantage of involving end users in continuity planning is that they:

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

Answer: A

NEW QUESTION 150
- (Exam Topic 3)
Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

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

Answer: A

NEW QUESTION 155
- (Exam Topic 3)
An organization is considering outsourcing user administration controls tor a critical system. The potential vendor has offered to perform quarterly sett-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to me risk practitioner?

A. The controls may not be properly tested
B. The vendor will not ensure against control failure
C. The vendor will not achieve best practices
D. Lack of a risk-based approach to access control

Answer: A

NEW QUESTION 159
- (Exam Topic 3)
A risk practitioner observed Vial a high number of pokey exceptions were approved by senior management. Which of the following is the risk practitioner's BEST course of action to determine root cause?

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

Answer: C

NEW QUESTION 164
- (Exam Topic 3)
Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:

A. a threat.
B. a vulnerability.
C. an impact
D. a control.

Answer: B

NEW QUESTION 167
- (Exam Topic 3)
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 168
- (Exam Topic 3)
When of the following standard operating procedure (SOP) statements BEST illustrates appropriate risk register maintenance?

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

Answer: C

NEW QUESTION 171
- (Exam Topic 3)
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 176
- (Exam Topic 3)
Which of the following is MOST important for an organization to update following a change in legislation requiring notification to individuals impacted by data

breaches?

A. Insurance coverage
B. Security awareness training
C. Policies and standards
D. Risk appetite and tolerance

Answer: C

NEW QUESTION 179
- (Exam Topic 3)
Which of the following is the MOST appropriate action when a tolerance threshold is exceeded?

A. Communicate potential impact to decision makers.
B. Research the root cause of similar incidents.
C. Verify the response plan is adequate.
D. Increase human resources to respond in the interim.

Answer: A

NEW QUESTION 183
- (Exam Topic 3)
it was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern1?

A. The underutilization of the replicated Iink
B. The cost of recovering the data
C. The lack of integrity of data
D. The loss of data confidentiality

Answer: C

NEW QUESTION 188
- (Exam Topic 3)
Which of The following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?

A. Perform a post-implementation review.
B. Conduct user acceptance testing.
C. Review the key performance indicators (KPIs).
D. Interview process owners.

Answer: C

NEW QUESTION 190
- (Exam Topic 3)
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 195
- (Exam Topic 3)
Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?

A. Fiscal management practices
B. Business maturity
C. Budget for implementing security
D. Management culture

Answer: D

NEW QUESTION 198
- (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 199

- (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 202
- (Exam Topic 3)
Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?

A. A decrease in the number of critical assets covered by risk thresholds
B. An Increase In the number of risk threshold exceptions
C. An increase in the number of change events pending management review
D. A decrease In the number of key performance indicators (KPIs)

Answer: B

NEW QUESTION 204
- (Exam Topic 3)
What is the PRIMARY reason an organization should include background checks on roles with elevated access to production as part of its hiring process?

A. Reduce internal threats
B. Reduce exposure to vulnerabilities
C. Eliminate risk associated with personnel
D. Ensure new hires have the required skills

Answer: C

NEW QUESTION 207
- (Exam Topic 3)
Which of the following sources is MOST relevant to reference when updating security awareness training materials?

A. Risk management framework
B. Risk register
C. Global security standards
D. Recent security incidents reported by competitors

Answer: B

NEW QUESTION 210
- (Exam Topic 3)
Which of the following BEST informs decision-makers about the value of a notice and consent control for the collection of personal information?

A. A comparison of the costs of notice and consent control options
B. Examples of regulatory fines incurred by industry peers for noncompliance
C. A report of critical controls showing the importance of notice and consent
D. A cost-benefit analysis of the control versus probable legal action

Answer: D

NEW QUESTION 211
- (Exam Topic 3)
Which of the following is the MOST important component in a risk treatment plan?

A. Technical details
B. Target completion date
C. Treatment plan ownership
D. Treatment plan justification

Answer: D

NEW QUESTION 216
- (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 217
- (Exam Topic 3)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

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

Answer: C

NEW QUESTION 219
- (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 220
- (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 221
- (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 226
- (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 230
- (Exam Topic 3)
Which of the following will BEST help to ensure implementation of corrective action plans?

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

Answer: B

NEW QUESTION 234
- (Exam Topic 3)
Which of the following is MOST helpful in aligning IT risk with business objectives?

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

Answer: C

NEW QUESTION 236
- (Exam Topic 3)
Which key performance efficiency IKPI) BEST measures the effectiveness of an organization's disaster recovery program?

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

Answer: D

NEW QUESTION 240
- (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 244
- (Exam Topic 3)
Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

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

Answer: D

NEW QUESTION 247
- (Exam Topic 3)
An organization automatically approves exceptions to security policies on a recurring basis. This practice is MOST likely the result of:

A. a lack of mitigating actions for identified risk
B. decreased threat levels
C. ineffective service delivery
D. ineffective IT governance

Answer: D

NEW QUESTION 248
- (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 251
- (Exam Topic 3)
Which of the following is MOST important information to review when developing plans for using emerging technologies?

A. Existing IT environment
B. IT strategic plan
C. Risk register
D. Organizational strategic plan

Answer: D

NEW QUESTION 252
- (Exam Topic 3)
An organization is considering the adoption of an aggressive business strategy to achieve desired growth From a risk management perspective what should the risk practitioner do NEXT?

A. Identify new threats resorting from the new business strategy
B. Update risk awareness training to reflect current levels of risk appetite and tolerance
C. Inform the board of potential risk scenarios associated with aggressive business strategies
D. Increase the scale for measuring impact due to threat materialization

Answer: A

NEW QUESTION 254
- (Exam Topic 3)
A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:

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

Answer: C

NEW QUESTION 258
- (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 260
- (Exam Topic 3)
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

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

Answer: D

NEW QUESTION 262
- (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 264
- (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 266
- (Exam Topic 3)
An organization wants to grant remote access to a system containing sensitive data to an overseas third party. Which of the following should be of GREATEST concern to management?

A. Transborder data transfer restrictions
B. Differences in regional standards
C. Lack of monitoring over vendor activities
D. Lack of after-hours incident management support

Answer: C

NEW QUESTION 267
- (Exam Topic 3)
When performing a risk assessment of a new service to support a ewe Business process. which of the following should be done FRST10 ensure continuity of operations?

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

Answer: A

NEW QUESTION 271
- (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 276
- (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 280
- (Exam Topic 3)
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 281
- (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 283
- (Exam Topic 3)
Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?

A. KPIs measure manual controls, while KCIs measure automated controls.
B. KPIs and KCIs both contribute to understanding of control effectiveness.
C. A robust KCI program will replace the need to measure KPIs.
D. KCIs are applied at the operational level while KPIs are at the strategic level.

Answer: B

NEW QUESTION 284
- (Exam Topic 3)
Which of the following is MOST important to compare against the corporate risk profile?

A. Industry benchmarks
B. Risk tolerance
C. Risk appetite
D. Regulatory compliance

Answer:

D

NEW QUESTION 288
- (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 289
- (Exam Topic 3)
An organizations chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

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

Answer: A

NEW QUESTION 293
- (Exam Topic 3)
When developing a new risk register, a risk practitioner should focus on which of the following risk management activities?

A. Risk management strategy planning
B. Risk monitoring and control
C. Risk identification
D. Risk response planning

Answer: C

NEW QUESTION 294
- (Exam Topic 3)
The PRIMARY benefit associated with key risk indicators (KRIs) is that they:

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

Answer: D

NEW QUESTION 299
- (Exam Topic 3)
An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?

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

Answer: B

NEW QUESTION 304
- (Exam Topic 3)
Which of the following statements describes the relationship between key risk indicators (KRIs) and key control indicators (KCIs)?

A. KRI design must precede definition of KCIs.
B. KCIs and KRIs are independent indicators and do not impact each other.
C. A decreasing trend of KRI readings will lead to changes to KCIs.
D. Both KRIs and KCIs provide insight to potential changes in the level of risk.

Answer: A

NEW QUESTION 309
- (Exam Topic 3)
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 314
- (Exam Topic 3)
A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

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

Answer: D

NEW QUESTION 315
- (Exam Topic 3)
While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

A. review and update the policies to align with industry standards.
B. determine that the policies should be updated annually.
C. report that the policies are adequate and do not need to be updated frequently.
D. review the policies against current needs to determine adequacy.

Answer: D

NEW QUESTION 317
- (Exam Topic 3)
Legal and regulatory risk associated with business conducted over the Internet is driven by:

A. the jurisdiction in which an organization has its principal headquarters
B. international law and a uniform set of regulations.
C. the laws and regulations of each individual country
D. international standard-setting bodies.

Answer: C

NEW QUESTION 320
- (Exam Topic 3)
Which of the following is the MOST effective way to incorporate stakeholder concerns when developing risk scenarios?

A. Evaluating risk impact
B. Establishing key performance indicators (KPIs)
C. Conducting internal audits
D. Creating quarterly risk reports

Answer: A

NEW QUESTION 325
- (Exam Topic 3)
An organization control environment is MOST effective when:

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

Answer: B

NEW QUESTION 327
- (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 328
- (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 329
- (Exam Topic 3)
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 330
- (Exam Topic 3)
An IT risk practitioner has been asked to regularly report on the overall status and effectiveness of the IT risk management program. Which of the following is MOST useful for this purpose?

A. Balanced scorecard
B. Capability maturity level
C. Internal audit plan
D. Control self-assessment (CSA)

Answer: A

NEW QUESTION 335
- (Exam Topic 3)
A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

A. Identify changes in risk factors and initiate risk reviews.
B. Engage an external consultant to redesign the risk management process.
C. Outsource the process for updating the risk register.
D. Implement a process improvement and replace the old risk register.

Answer: A

NEW QUESTION 338
- (Exam Topic 3)
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 341
- (Exam Topic 3)
Which of the following is MOST useful when communicating risk to management?

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

Answer: C

NEW QUESTION 342
- (Exam Topic 3)
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 345
- (Exam Topic 3)
Which of the following is the STRONGEST indication an organization has ethics management issues?

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

Answer: A

NEW QUESTION 346
- (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 349
- (Exam Topic 3)
Which of the following is the BEST method of creating risk awareness in an organization?

A. Marking the risk register available to project stakeholders
B. Ensuring senior management commitment to risk training
C. Providing regular communication to risk managers
D. Appointing the risk manager from the business units

Answer: B

NEW QUESTION 352
- (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 357
- (Exam Topic 3)
A violation of segregation of duties is when the same:

A. user requests and tests the change prior to production.
B. user authorizes and monitors the change post-implementation.
C. programmer requests and tests the change prior to production.
D. programmer writes and promotes code into production.

Answer: D

NEW QUESTION 360
- (Exam Topic 3)
Which of the following would BEST mitigate an identified risk scenario?

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

Answer: C

NEW QUESTION 364
- (Exam Topic 3)
An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

A. Management may be unable to accurately evaluate the risk profile.
B. Resources may be inefficiently allocated.
C. The same risk factor may be identified in multiple areas.
D. Multiple risk treatment efforts may be initiated to treat a given risk.

Answer: B

NEW QUESTION 367
- (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 368
- (Exam Topic 3)
For a large software development project, risk assessments are MOST effective when performed:

A. before system development begins.
B. at system development.
C. at each stage of the system development life cycle (SDLC).
D. during the development of the business case.

Answer: C

NEW QUESTION 371
- (Exam Topic 3)
Which of the following provides the BEST measurement of an organization's risk management maturity level?

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

Answer: C

NEW QUESTION 376
- (Exam Topic 3)
Which of the following is the MOST effective control to ensure user access is maintained on a least-privilege basis?

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

Answer: B

NEW QUESTION 377
- (Exam Topic 3)
An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate tins risk?

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

Answer: C

NEW QUESTION 381
- (Exam Topic 2)
A new policy has been published to forbid copying of data onto removable media. Which type of control has been implemented?

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

Answer: C

NEW QUESTION 383
- (Exam Topic 2)
Which of the following is the PRIMARY role of the board of directors in corporate risk governance?

A. Approving operational strategies and objectives
B. Monitoring the results of actions taken to mitigate risk

C. Ensuring the effectiveness of the risk management program
D. Ensuring risk scenarios are identified and recorded in the risk register

Answer: C

NEW QUESTION 386
- (Exam Topic 2)
An organization's internal audit department is considering the implementation of robotics process automation (RPA) to automate certain continuous auditing tasks. Who would own the risk associated with ineffective design of the software bots?

A. Lead auditor
B. Project manager
C. Chief audit executive (CAE)
D. Chief information officer (CIO)

Answer: C

NEW QUESTION 388
- (Exam Topic 2)
Which of the following is a crucial component of a key risk indicator (KRI) to ensure appropriate action is taken to mitigate risk?

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

Answer: D

NEW QUESTION 390
- (Exam Topic 2)
The maturity of an IT risk management program is MOST influenced by:

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

Answer: A

NEW QUESTION 393
- (Exam Topic 2)
Which of the following is MOST influential when management makes risk response decisions?

A. Risk appetite
B. Audit risk
C. Residual risk
D. Detection risk

Answer: A

NEW QUESTION 396
- (Exam Topic 2)
Which of the following is performed after a risk assessment is completed?

A. Defining risk taxonomy
B. Identifying vulnerabilities
C. Conducting an impact analysis
D. Defining risk response options

Answer: C

NEW QUESTION 397
- (Exam Topic 2)
Which of the following is MOST helpful to review when identifying risk scenarios associated with the adoption of Internet of Things (loT) technology in an organization?

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

Answer: B

NEW QUESTION 398
- (Exam Topic 2)

The MOST important reason to aggregate results from multiple risk assessments on interdependent information systems is to:

A. establish overall impact to the organization
B. efficiently manage the scope of the assignment
C. identify critical information systems
D. facilitate communication to senior management

Answer: A

NEW QUESTION 399
- (Exam Topic 2)
Of the following, who should be responsible for determining the inherent risk rating of an application?

A. Application owner
B. Senior management
C. Risk practitioner
D. Business process owner

Answer: C

NEW QUESTION 402
- (Exam Topic 2)
A risk practitioner is reviewing a vendor contract and finds there is no clause to control privileged access to the organization's systems by vendor employees. Which of the following is the risk practitioner's BEST course of action?

A. Contact the control owner to determine if a gap in controls exists.
B. Add this concern to the risk register and highlight it for management review.
C. Report this concern to the contracts department for further action.
D. Document this concern as a threat and conduct an impact analysis.

Answer: D

NEW QUESTION 405
- (Exam Topic 2)
Which of the following criteria is MOST important when developing a response to an attack that would compromise data?

A. The recovery time objective (RTO)
B. The likelihood of a recurring attack
C. The organization's risk tolerance
D. The business significance of the information

Answer: D

NEW QUESTION 408
- (Exam Topic 2)
Which of the following is the MAIN benefit of involving stakeholders in the selection of key risk indicators (KRIs)?

A. Improving risk awareness
B. Obtaining buy-in from risk owners
C. Leveraging existing metrics
D. Optimizing risk treatment decisions

Answer: B

NEW QUESTION 411
- (Exam Topic 2)
After mapping generic risk scenarios to organizational security policies, the NEXT course of action should be to:

A. record risk scenarios in the risk register for analysis.
B. validate the risk scenarios for business applicability.
C. reduce the number of risk scenarios to a manageable set.
D. perform a risk analysis on the risk scenarios.

Answer: B

NEW QUESTION 413
- (Exam Topic 2)
Which of the following is MOST important when developing risk scenarios?

A. The scenarios are based on industry best practice.
B. The scenarios focus on current vulnerabilities.
C. The scenarios are relevant to the organization.
D. The scenarios include technical consequences.

Answer: C

NEW QUESTION 418
- (Exam Topic 2)
Which of the following is the BEST way to identify changes in the risk profile of an organization?

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

Answer: D

NEW QUESTION 420
- (Exam Topic 2)
A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?

A. Recommend allowing the new usage based on prior approval.
B. Request a new third-party review.
C. Request revalidation of the original use case.
D. Assess the risk associated with the new use case.

Answer: D

NEW QUESTION 424
- (Exam Topic 2)
The PRIMARY purpose of using control metrics is to evaluate the:

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

Answer: C

NEW QUESTION 428
- (Exam Topic 2)
Which of the following would BEST help secure online financial transactions from improper users?

A. Review of log-in attempts
B. Multi-level authorization
C. Periodic review of audit trails
D. Multi-factor authentication

Answer: D

NEW QUESTION 431
- (Exam Topic 2)
After identifying new risk events during a project, the project manager s NEXT step should be to:

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

Answer: B

NEW QUESTION 436
- (Exam Topic 2)
Which of the following should be considered FIRST when assessing risk associated with the adoption of emerging technologies?

A. Organizational strategy
B. Cost-benefit analysis
C. Control self-assessment (CSA)
D. Business requirements

Answer: A

NEW QUESTION 441
- (Exam Topic 2)
Which of the following BEST helps to balance the costs and benefits of managing IT risk?

A. Prioritizing risk responses
B. Evaluating risk based on frequency and probability
C. Considering risk factors that can be quantified
D. Managing the risk by using controls

Answer:

A

NEW QUESTION 446
- (Exam Topic 2)
An organization is planning to outsource its payroll function to an external service provider Which of the following should be the MOST important consideration when selecting the provider?

A. Disaster recovery plan (DRP) of the system
B. Right to audit the provider
C. Internal controls to ensure data privacy
D. Transparency of key performance indicators (KPIs)

Answer: B

NEW QUESTION 449
- (Exam Topic 2)
It is MOST important to the effectiveness of an IT risk management function that the associated processes are:

A. aligned to an industry-accepted framework.
B. reviewed and approved by senior management.
C. periodically assessed against regulatory requirements.
D. updated and monitored on a continuous basis.

Answer: C

NEW QUESTION 451
- (Exam Topic 2)
During the control evaluation phase of a risk assessment, it is noted that multiple controls are ineffective. Which of the following should be the risk practitioner's FIRST course of action?

A. Recommend risk remediation of the ineffective controls.
B. Compare the residual risk to the current risk appetite.
C. Determine the root cause of the control failures.
D. Escalate the control failures to senior management.

Answer: C

NEW QUESTION 455
- (Exam Topic 2)
Which of the following is the MOST effective way to integrate business risk management with IT operations?

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

Answer: D

NEW QUESTION 458
- (Exam Topic 2)
When establishing leading indicators for the information security incident response process it is MOST important to consider the percentage of reported incidents:

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

Answer: C

NEW QUESTION 461
- (Exam Topic 2)
Which of the following BEST contributes to the implementation of an effective risk response action plan?

A. An IT tactical plan
B. Disaster recovery and continuity testing
C. Assigned roles and responsibilities
D. A business impact analysis

Answer: C

NEW QUESTION 465
- (Exam Topic 2)
Which of the following will BEST ensure that information security risk factors are mitigated when developing in-house applications?

A. Identify information security controls in the requirements analysis
B. Identify key risk indicators (KRIs) as process output.

C. Design key performance indicators (KPIs) for security in system specifications.
D. Include information security control specifications in business cases.

Answer: D

NEW QUESTION 470
- (Exam Topic 2)
Prior to selecting key performance indicators (KPIs), itis MOST important to ensure:

A. trending data is available.
B. process flowcharts are current.
C. measurement objectives are defined.
D. data collection technology is available.

Answer: C

NEW QUESTION 475
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?

A. Percentage of vulnerabilities remediated within the agreed service level
B. Number of vulnerabilities identified during the period
C. Number of vulnerabilities re-opened during the period
D. Percentage of vulnerabilities escalated to senior management

Answer: A

NEW QUESTION 478
- (Exam Topic 2)
What should a risk practitioner do FIRST upon learning a risk treatment owner has implemented a different control than what was specified in the IT risk action plan?

A. Seek approval from the control owner.
B. Update the action plan in the risk register.
C. Reassess the risk level associated with the new control.
D. Validate that the control has an established testing method.

Answer: C

NEW QUESTION 480
- (Exam Topic 2)
It is MOST important for a risk practitioner to have an awareness of an organization s processes in order to:

A. perform a business impact analysis.
B. identify potential sources of risk.
C. establish risk guidelines.
D. understand control design.

Answer: B

NEW QUESTION 484
- (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 489
- (Exam Topic 2)
Which of the following is the MOST important consideration when identifying stakeholders to review risk scenarios developed by a risk analyst? The reviewers are:

A. accountable for the affected processes.
B. members of senior management.
C. authorized to select risk mitigation options.
D. independent from the business operations.

Answer: D

NEW QUESTION 494
- (Exam Topic 2)
Which of the following is MOST helpful in developing key risk indicator (KRI) thresholds?

A. Loss expectancy information
B. Control performance predictions
C. IT service level agreements (SLAs)
D. Remediation activity progress

Answer: A

NEW QUESTION 496
- (Exam Topic 2)
A risk practitioner is reporting on an increasing trend of ransomware attacks in the industry. Which of the following information is MOST important to include to enable an informed response decision by key stakeholders?

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

Answer: D

NEW QUESTION 498
- (Exam Topic 2)
Which of the following is the GREATEST concern associated with business end users developing their own applications on end user spreadsheets and database programs?

A. An IT project manager is not assigned to oversee development.
B. Controls are not applied to the applications.
C. There is a lack of technology recovery options.
D. The applications are not captured in the risk profile.

Answer: C

NEW QUESTION 503
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to update when a software upgrade renders an existing key control ineffective?

A. Audit engagement letter
B. Risk profile
C. IT risk register
D. Change control documentation

Answer: C

NEW QUESTION 505
- (Exam Topic 2)
Which of the following is MOST helpful to management when determining the resources needed to mitigate a risk?

A. An internal audit
B. A heat map
C. A business impact analysis (BIA)
D. A vulnerability report

Answer: C

NEW QUESTION 509
- (Exam Topic 2)
Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

A. Risk tolerance
B. Risk appetite
C. Risk awareness
D. Risk policy

Answer: B

NEW QUESTION 510
- (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 514
- (Exam Topic 2)
Which of the following is the PRIMARY objective for automating controls?

A. Improving control process efficiency
B. Facilitating continuous control monitoring
C. Complying with functional requirements
D. Reducing the need for audit reviews

Answer: A

NEW QUESTION 517
- (Exam Topic 2)
Which of the following should management consider when selecting a risk mitigation option?

A. Maturity of the enterprise architecture
B. Cost of control implementation
C. Reliability of key performance indicators (KPIs)
D. Reliability of key risk indicators (KPIs)

Answer: B

NEW QUESTION 518
- (Exam Topic 2)
Which of the following is the MOST important data attribute of key risk indicators (KRIs)?

A. The data is measurable.
B. The data is calculated continuously.
C. The data is relevant.
D. The data is automatically produced.

Answer: C

NEW QUESTION 521
- (Exam Topic 2)
Which of the following will BEST help to ensure that information system controls are effective?

A. Responding promptly to control exceptions
B. Implementing compensating controls
C. Testing controls periodically
D. Automating manual controls

Answer: C

NEW QUESTION 523
- (Exam Topic 2)
The PRIMARY reason for establishing various Threshold levels for a set of key risk indicators (KRIs) is to:

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

Answer: B

NEW QUESTION 527
- (Exam Topic 2)
A control owner identifies that the organization's shared drive contains personally identifiable information (Pll) that can be accessed by all personnel. Which of the following is the MOST effective risk response?

A. Protect sensitive information with access controls.
B. Implement a data loss prevention (DLP) solution.
C. Re-communicate the data protection policy.
D. Implement a data encryption solution.

Answer: A

NEW QUESTION 528
- (Exam Topic 2)
The MAIN goal of the risk analysis process is to determine the:

A. potential severity of impact
B. frequency and magnitude of loss
C. control deficiencies
D. threats and vulnerabilities

Answer:

B

NEW QUESTION 530
- (Exam Topic 2)
An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

A. IT infrastructure head
B. Human resources head
C. Supplier management head
D. Application development head

Answer: B

NEW QUESTION 533
- (Exam Topic 2)
Which of the following is the MOST important objective of embedding risk management practices into the initiation phase of the project management life cycle?

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

Answer: B

NEW QUESTION 534
- (Exam Topic 2)
Which of the following is the BEST course of action when risk is found to be above the acceptable risk appetite?

A. Review risk tolerance levels
B. Maintain the current controls.
C. Analyze the effectiveness of controls.
D. Execute the risk response plan

Answer: D

NEW QUESTION 538
- (Exam Topic 2)
Which of the following BEST indicates that an organizations risk management program is effective?

A. Fewer security incidents have been reported.
B. The number of audit findings has decreased.
C. Residual risk is reduced.
D. inherent risk Is unchanged.

Answer: C

NEW QUESTION 542
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of a control monitoring program?

A. Time between control failure and failure detection
B. Number of key controls as a percentage of total control count
C. Time spent on internal control assessment reviews
D. Number of internal control failures within the measurement period

Answer: A

NEW QUESTION 547
- (Exam Topic 2)
Which of the following would MOST likely cause a risk practitioner to reassess risk scenarios?

A. A change in the risk management policy
B. A major security incident
C. A change in the regulatory environment
D. An increase in intrusion attempts

Answer: C

NEW QUESTION 548
- (Exam Topic 2)
For no apparent reason, the time required to complete daily processing for a legacy application is approaching a risk threshold. Which of the following activities should be performed FIRST?

A. Temporarily increase the risk threshold.
B. Suspend processing to investigate the problem.
C. Initiate a feasibility study for a new application.

D. Conduct a root-cause analysis.

Answer: D

NEW QUESTION 550
- (Exam Topic 2)
A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (Pll). Which of the following will MOST likely outcome for an organization affected by the new law?

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

Answer: B

NEW QUESTION 551
- (Exam Topic 2)
The risk associated with inadvertent disclosure of database records from a public cloud service provider (CSP) would MOST effectively be reduced by:

A. encrypting the data
B. including a nondisclosure clause in the CSP contract
C. assessing the data classification scheme
D. reviewing CSP access privileges

Answer: A

NEW QUESTION 555
- (Exam Topic 2)
Which of the following is MOST important when discussing risk within an organization?

A. Adopting a common risk taxonomy
B. Using key performance indicators (KPIs)
C. Creating a risk communication policy
D. Using key risk indicators (KRIs)

Answer: A

NEW QUESTION 556
- (Exam Topic 2)
To help ensure all applicable risk scenarios are incorporated into the risk register, it is MOST important to review the:

A. risk mitigation approach
B. cost-benefit analysis.
C. risk assessment results.
D. vulnerability assessment results

Answer: C

NEW QUESTION 560
- (Exam Topic 2)
An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

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

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

Answer: A

NEW QUESTION 562
- (Exam Topic 2)
Which of the following is the MOST effective way to help ensure an organization's current risk scenarios are relevant?

A. Adoption of industry best practices
B. Involvement of stakeholders in risk assessment
C. Review of risk scenarios by independent parties
D. Documentation of potential risk in business cases

Answer: B

NEW QUESTION 566
- (Exam Topic 2)
The MOST essential content to include in an IT risk awareness program is how to:

A. populate risk register entries and build a risk profile for management reporting.
B. prioritize IT-related actions by considering risk appetite and risk tolerance.
C. define the IT risk framework for the organization.
D. comply with the organization's IT risk and information security policies.

Answer: D

NEW QUESTION 569
- (Exam Topic 2)
Which of the following is MOST helpful in identifying gaps between the current and desired state of the IT risk environment?

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

Answer: C

NEW QUESTION 572
- (Exam Topic 2)
The MOST significant benefit of using a consistent risk ranking methodology across an organization is that it enables:

A. allocation of available resources
B. clear understanding of risk levels
C. assignment of risk to the appropriate owners
D. risk to be expressed in quantifiable terms

Answer: B

NEW QUESTION 573
- (Exam Topic 2)
Which of the following controls would BEST reduce the likelihood of a successful network attack through social engineering?

A. Automated controls
B. Security awareness training
C. Multifactor authentication
D. Employee sanctions

Answer: B

NEW QUESTION 578
- (Exam Topic 2)
Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?

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

Answer: A

NEW QUESTION 582
- (Exam Topic 2)
Mitigating technology risk to acceptable levels should be based PRIMARILY upon:

A. organizational risk appetite.
B. business sector best practices.
C. business process requirements.
D. availability of automated solutions

Answer: C

NEW QUESTION 587
- (Exam Topic 2)
A new regulator/ requirement imposes severe fines for data leakage involving customers' personally identifiable information (Pll). The risk practitioner has recommended avoiding the risk. Which of the following actions would BEST align with this recommendation?

A. Reduce retention periods for Pll data.
B. Move Pll to a highly-secured outsourced site.

C. Modify business processes to stop collecting Pll.
D. Implement strong encryption for Pll.

Answer: C

NEW QUESTION 589
- (Exam Topic 2)
What are the MOST important criteria to consider when developing a data classification scheme to facilitate risk assessment and the prioritization of risk mitigation activities?

A. Mitigation and control value
B. Volume and scope of data generated daily
C. Business criticality and sensitivity
D. Recovery point objective (RPO) and recovery time objective (RTO)

Answer: C

NEW QUESTION 594
- (Exam Topic 2)
Who is PRIMARILY accountable for risk treatment decisions?

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

Answer: A

NEW QUESTION 597
- (Exam Topic 2)
A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

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

Answer: C

NEW QUESTION 599
- (Exam Topic 2)
Which of the following is the BEST approach for determining whether a risk action plan is effective?

A. Comparing the remediation cost against budget
B. Assessing changes in residual risk
C. Assessing the inherent risk
D. Monitoring changes of key performance indicators (KPIs)

Answer: B

NEW QUESTION 604
- (Exam Topic 2)
Which of The following would offer the MOST insight with regard to an organization's risk culture?

A. Risk management procedures
B. Senior management interviews
C. Benchmark analyses
D. Risk management framework

Answer: B

NEW QUESTION 605
- (Exam Topic 2)
Which of the following would MOST likely result in updates to an IT risk appetite statement?

A. External audit findings
B. Feedback from focus groups
C. Self-assessment reports
D. Changes in senior management

Answer: D

NEW QUESTION 606
- (Exam Topic 2)

Which of the following MOST effectively limits the impact of a ransomware attack?

A. Cyber insurance
B. Cryptocurrency reserve
C. Data backups
D. End user training

Answer: C

NEW QUESTION 609
- (Exam Topic 2)
What is the GREATEST concern with maintaining decentralized risk registers instead of a consolidated risk register?

A. Aggregated risk may exceed the enterprise's risk appetite and tolerance.
B. Duplicate resources may be used to manage risk registers.
C. Standardization of risk management practices may be difficult to enforce.
D. Risk analysis may be inconsistent due to non-uniform impact and likelihood scales.

Answer: C

NEW QUESTION 611
- (Exam Topic 2)
Which of the following is the BEST approach for performing a business impact analysis (BIA) of a supply-chain management application?

A. Reviewing the organization's policies and procedures
B. Interviewing groups of key stakeholders
C. Circulating questionnaires to key internal stakeholders
D. Accepting IT personnel s view of business issues

Answer: B

NEW QUESTION 616
- (Exam Topic 2)
Which of the following resources is MOST helpful when creating a manageable set of IT risk scenarios?

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

Answer: B

NEW QUESTION 619
- (Exam Topic 2)
Which of the following is the MOST important reason to create risk scenarios?

A. To assist with risk identification
B. To determine risk tolerance
C. To determine risk appetite
D. To assist in the development of risk responses

Answer: A

NEW QUESTION 621
- (Exam Topic 2)
Which of the following is MOST important to understand when developing key risk indicators (KRIs)?

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

Answer: B

NEW QUESTION 622
- (Exam Topic 2)
Which of the following provides the MOST important information to facilitate a risk response decision?

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

Answer: B

NEW QUESTION 627

- (Exam Topic 2)
A risk practitioner learns that the organization s industry is experiencing a trend of rising security incidents. Which of the following is the BEST course of action?

A. Evaluate the relevance of the evolving threats.
B. Review past internal audit results.
C. Respond to organizational security threats.
D. Research industry published studies.

Answer: A

NEW QUESTION 628
- (Exam Topic 2)
A payroll manager discovers that fields in certain payroll reports have been modified without authorization. Which of the following control weaknesses could have contributed MOST to this problem?

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

Answer: B

NEW QUESTION 630
- (Exam Topic 2)
Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

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

Answer: D

NEW QUESTION 632
- (Exam Topic 2)
The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

A. ensure policy and regulatory compliance.
B. assess the proliferation of new threats.
C. verify Internet firewall control settings.
D. identify vulnerabilities in the system.

Answer: C

NEW QUESTION 637
- (Exam Topic 2)
What should be the PRIMARY objective for a risk practitioner performing a post-implementation review of an IT risk mitigation project?

A. Documenting project lessons learned
B. Validating the risk mitigation project has been completed
C. Confirming that the project budget was not exceeded
D. Verifying that the risk level has been lowered

Answer: A

NEW QUESTION 642
- (Exam Topic 2)
The risk associated with data loss from a website which contains sensitive customer information is BEST owned by:

A. the third-party website manager
B. the business process owner
C. IT security
D. the compliance manager

Answer: B

NEW QUESTION 644
- (Exam Topic 2)
An organization has introduced risk ownership to establish clear accountability for each process. To ensure effective risk ownership, it is MOST important that:

A. senior management has oversight of the process.
B. process ownership aligns with IT system ownership.
C. segregation of duties exists between risk and process owners.
D. risk owners have decision-making authority.

Answer: A

NEW QUESTION 648
- (Exam Topic 2)
Which of the following is MOST helpful in determining the effectiveness of an organization's IT risk mitigation efforts?

A. Assigning identification dates for risk scenarios in the risk register
B. Updating impact assessments for risk scenario
C. Verifying whether risk action plans have been completed
D. Reviewing key risk indicators (KRIS)

Answer: D

NEW QUESTION 651
- (Exam Topic 2)
A risk owner has accepted a high-impact risk because the control was adversely affecting process efficiency. Before updating the risk register, it is MOST important for the risk practitioner to:

A. ensure suitable insurance coverage is purchased.
B. negotiate with the risk owner on control efficiency.
C. reassess the risk to confirm the impact.
D. obtain approval from senior management.

Answer: D

NEW QUESTION 653
- (Exam Topic 2)
An upward trend in which of the following metrics should be of MOST concern?

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

Answer: C

NEW QUESTION 654
- (Exam Topic 2)
An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:

A. identifying risk scenarios.
B. determining the risk strategy.
C. calculating impact and likelihood.
D. completing the controls catalog.

Answer: A

NEW QUESTION 657
- (Exam Topic 2)
Which of the following would prompt changes in key risk indicator {KRI) thresholds?

A. Changes to the risk register
B. Changes in risk appetite or tolerance
C. Modification to risk categories
D. Knowledge of new and emerging threats

Answer: B

NEW QUESTION 662
- (Exam Topic 2)
The PRIMARY objective of The board of directors periodically reviewing the risk profile is to help ensure:

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

Answer: A

NEW QUESTION 667
- (Exam Topic 2)
IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

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

Answer: D

NEW QUESTION 671
- (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 676
- (Exam Topic 2)
What can be determined from the risk scenario chart?

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

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

Answer: A

NEW QUESTION 677
- (Exam Topic 1)
Which of the following elements of a risk register is MOST likely to change as a result of change in management's risk appetite?

A. Key risk indicator (KRI) thresholds
B. Inherent risk
C. Risk likelihood and impact
D. Risk velocity

Answer: A

NEW QUESTION 678
- (Exam Topic 3)
Which of the following should be the GREATEST concern for an organization that uses open source software applications?

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

Answer: A

NEW QUESTION 681
- (Exam Topic 3)
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 683
- (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 684
- (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 686
- (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 690
- (Exam Topic 3)
A risk practitioner is preparing a report to communicate changes in the risk and control environment. The BEST way to engage stakeholder attention is to:

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

Answer: B

NEW QUESTION 693
- (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 694
- (Exam Topic 3)
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?

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

Answer: C

NEW QUESTION 697
- (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 701
- (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 705
- (Exam Topic 3)
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 708
- (Exam Topic 3)
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

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

Answer: A

NEW QUESTION 712
- (Exam Topic 3)
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 716
- (Exam Topic 3)
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: D

NEW QUESTION 719
- (Exam Topic 3)
A cote data center went offline abruptly for several hours affecting many transactions across multiple locations. Which of the to" owing would provide the MOST useful information to determine mitigating controls?

A. Forensic analysis
B. Risk assessment
C. Root cause analysis
D. Business impact analysis (BIA)

Answer: A

NEW QUESTION 724
- (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 728
- (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 731
- (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 733
- (Exam Topic 3)
Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

A. Internal auditor
B. Asset owner
C. Finance manager
D. Control owner

Answer: B

NEW QUESTION 736
- (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 737
- (Exam Topic 3)
Who is BEST suited to determine whether a new control properly mitigates data loss risk within a system?

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

Answer: B

NEW QUESTION 742
- (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 745
- (Exam Topic 3)
Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

A. Complete an offsite business continuity exercise.
B. Conduct a compliance check against standards.
C. Perform a vulnerability assessment.
D. Measure the change in inherent risk.

Answer: C

NEW QUESTION 750
- (Exam Topic 3)
Which of the following is the BEST approach to mitigate the risk associated with a control deficiency?

A. Perform a business case analysis
B. Implement compensating controls.
C. Conduct a control sell-assessment (CSA)
D. Build a provision for risk

Answer: C

NEW QUESTION 753
- (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 755
- (Exam Topic 2)
Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?

A. Trends in IT resource usage
B. Trends in IT maintenance costs
C. Increased resource availability
D. Increased number of incidents

Answer: A

NEW QUESTION 756
- (Exam Topic 2)
A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 759
- (Exam Topic 2)
The MOST effective approach to prioritize risk scenarios is by:

A. assessing impact to the strategic plan.
B. aligning with industry best practices.
C. soliciting input from risk management experts.
D. evaluating the cost of risk response.

Answer: A

NEW QUESTION 762
- (Exam Topic 2)
During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?

A. Implement compensating controls to reduce residual risk
B. Escalate the issue to senior management
C. Discuss risk mitigation options with the risk owner.
D. Certify the control after documenting the concern.

Answer: A

NEW QUESTION 765
- (Exam Topic 2)
Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

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

Answer: B

NEW QUESTION 768

- (Exam Topic 2)
The FIRST task when developing a business continuity plan should be to:

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

Answer: B

NEW QUESTION 770
- (Exam Topic 2)
Which of the following is MOST important to review when determining whether a potential IT service provider's control environment is effective?

A. Independent audit report
B. Control self-assessment
C. MOST important to update when an
D. Service level agreements (SLAs)

Answer: A

NEW QUESTION 773
- (Exam Topic 2)
An external security audit has reported multiple findings related to control noncompliance. Which of the following would be MOST important for the risk practitioner to communicate to senior management?

A. A recommendation for internal audit validation
B. Plans for mitigating the associated risk
C. Suggestions for improving risk awareness training
D. The impact to the organization's risk profile

Answer: D

NEW QUESTION 778
- (Exam Topic 2)
An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?

A. Classification of the data
B. Type of device
C. Remote management capabilities
D. Volume of data

Answer: A

NEW QUESTION 782
- (Exam Topic 2)
Which of the following should a risk practitioner do FIRST when an organization decides to use a cloud service?

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

Answer: D

NEW QUESTION 787
- (Exam Topic 2)
An organization has raised the risk appetite for technology risk. The MOST likely result would be:

A. increased inherent risk.
B. higher risk management cost
C. decreased residual risk.
D. lower risk management cost.

Answer: D

NEW QUESTION 791
- (Exam Topic 2)
Which of the following is MOST likely to be impacted as a result of a new policy which allows staff members to remotely connect to the organization's IT systems via personal or public computers?

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

Answer: B

NEW QUESTION 792
- (Exam Topic 2)
Which of the following provides the MOST helpful information in identifying risk in an organization?

A. Risk registers
B. Risk analysis
C. Risk scenarios
D. Risk responses

Answer: C

NEW QUESTION 796
- (Exam Topic 2)
An organization has implemented a system capable of comprehensive employee monitoring. Which of the following should direct how the system is used?

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

Answer: D

NEW QUESTION 801
- (Exam Topic 2)
Which of the following will BEST help an organization evaluate the control environment of several third-party vendors?

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

Answer: B

NEW QUESTION 806
- (Exam Topic 2)
Which of the following BEST enables the risk profile to serve as an effective resource to support business objectives?

A. Engaging external risk professionals to periodically review the risk
B. Prioritizing global standards over local requirements in the risk profile
C. Updating the risk profile with risk assessment results
D. Assigning quantitative values to qualitative metrics in the risk register

Answer: C

NEW QUESTION 808
- (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 809
- (Exam Topic 2)
During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?

A. Communicate the decision to the risk owner for approval
B. Seek approval from the previous action plan manager.
C. Identify an owner for the new control.
D. Modify the action plan in the risk register.

Answer: A

NEW QUESTION 810
- (Exam Topic 2)
Implementing which of the following will BEST help ensure that systems comply with an established baseline before deployment?

A. Vulnerability scanning
B. Continuous monitoring and alerting

C. Configuration management
D. Access controls and active logging

Answer: C

NEW QUESTION 814
- (Exam Topic 2)
Which of the following risk register elements is MOST likely to be updated if the attack surface or exposure of an asset is reduced?

A. Likelihood rating
B. Control effectiveness
C. Assessment approach
D. Impact rating

Answer: A

NEW QUESTION 816
- (Exam Topic 2)
Which of the following should be initiated when a high number of noncompliant conditions are observed during review of a control procedure?

A. Disciplinary action
B. A control self-assessment
C. A review of the awareness program
D. Root cause analysis

Answer: D

NEW QUESTION 821
- (Exam Topic 2)
Which of the following would be a weakness in procedures for controlling the migration of changes to production libraries?

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

Answer: A

NEW QUESTION 826
- (Exam Topic 2)
Which of the following is MOST important to include in a Software as a Service (SaaS) vendor agreement?

A. An annual contract review
B. A service level agreement (SLA)
C. A requirement to adopt an established risk management framework
D. A requirement to provide an independent audit report

Answer: B

NEW QUESTION 830
- (Exam Topic 2)
An organization is planning to acquire a new financial system. Which of the following stakeholders would provide the MOST relevant information for analyzing the risk associated with the new IT solution?

A. Project sponsor
B. Process owner
C. Risk manager
D. Internal auditor

Answer: B

NEW QUESTION 833
- (Exam Topic 2)
Which of the following activities should be performed FIRST when establishing IT risk management processes?

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

Answer: D

NEW QUESTION 835
- (Exam Topic 1)
Which of the following would be a risk practitioners BEST recommendation for preventing cyber intrusion?

A. Establish a cyber response plan
B. Implement data loss prevention (DLP) tools.
C. Implement network segregation.
D. Strengthen vulnerability remediation efforts.

Answer: D

NEW QUESTION 836
- (Exam Topic 1)
An organization delegates its data processing to the internal IT team to manage information through its applications. Which of the following is the role of the internal IT team in this situation?

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

Answer: B

NEW QUESTION 839
- (Exam Topic 1)
Which of the following changes would be reflected in an organization's risk profile after the failure of a critical patch implementation?

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

Answer: D

NEW QUESTION 840
- (Exam Topic 1)
Which of the following is the BEST way to identify changes to the risk landscape?

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

Answer: C

NEW QUESTION 841
- (Exam Topic 1)
A risk practitioner has observed that there is an increasing trend of users sending sensitive information by email without using encryption. Which of the following would be the MOST effective approach to mitigate the risk associated with data loss?

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

Answer: C

NEW QUESTION 846
- (Exam Topic 1)
Which of the following will BEST mitigate the risk associated with IT and business misalignment?

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

Answer: D

NEW QUESTION 848
- (Exam Topic 1)
Which of the following is MOST helpful in identifying new risk exposures due to changes in the business environment?

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

Answer: B

NEW QUESTION 851

- (Exam Topic 1)
Which of the following would be the BEST recommendation if the level of risk in the IT risk profile has decreased and is now below management's risk appetite?

A. Optimize the control environment.
B. Realign risk appetite to the current risk level.
C. Decrease the number of related risk scenarios.
D. Reduce the risk management budget.

Answer: A

NEW QUESTION 855
- (Exam Topic 1)
Who is the MOST appropriate owner for newly identified IT risk?

A. The manager responsible for IT operations that will support the risk mitigation efforts
B. The individual with authority to commit organizational resources to mitigate the risk
C. A project manager capable of prioritizing the risk remediation efforts
D. The individual with the most IT risk-related subject matter knowledge

Answer: B

NEW QUESTION 858
- (Exam Topic 1)
A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:

A. identification.
B. treatment.
C. communication.
D. assessment

Answer: C

NEW QUESTION 861
- (Exam Topic 1)
Which of the following controls will BEST detect unauthorized modification of data by a database administrator?

A. Reviewing database access rights
B. Reviewing database activity logs
C. Comparing data to input records
D. Reviewing changes to edit checks

Answer: B

NEW QUESTION 866
- (Exam Topic 1)
Which of the following would be MOST important for a risk practitioner to provide to the internal audit department during the audit planning process?

A. Closed management action plans from the previous audit
B. Annual risk assessment results
C. An updated vulnerability management report
D. A list of identified generic risk scenarios

Answer: A

NEW QUESTION 870
- (Exam Topic 1)
A risk practitioner discovers several key documents detailing the design of a product currently in development have been posted on the Internet. What should be the risk practitioner's FIRST course of action?

A. invoke the established incident response plan.
B. Inform internal audit.
C. Perform a root cause analysis
D. Conduct an immediate risk assessment

Answer: A

NEW QUESTION 873
- (Exam Topic 1)
An unauthorized individual has socially engineered entry into an organization's secured physical premises. Which of the following is the BEST way to prevent future occurrences?

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

Answer: B

NEW QUESTION 878
- (Exam Topic 1)
A key risk indicator (KRI) is reported to senior management on a periodic basis as exceeding thresholds, but each time senior management has decided to take no action to reduce the risk. Which of the following is the MOST likely reason for senior management's response?

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

Answer: C

NEW QUESTION 882
- (Exam Topic 1)
Which of the following is the MOST important characteristic of an effective risk management program?

A. Risk response plans are documented
B. Controls are mapped to key risk scenarios.
C. Key risk indicators are defined.
D. Risk ownership is assigned

Answer: D

NEW QUESTION 887
- (Exam Topic 1)
An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?

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

Answer: B

NEW QUESTION 890
- (Exam Topic 1)
A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

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

Answer: A

NEW QUESTION 895
- (Exam Topic 1)
What is the BEST information to present to business control owners when justifying costs related to controls?

A. Loss event frequency and magnitude
B. The previous year's budget and actuals
C. Industry benchmarks and standards
D. Return on IT security-related investments

Answer: D

NEW QUESTION 897
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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