Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

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

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

Answer: C

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

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

Answer: B

NEW QUESTION 3
- (Exam Topic 4)
Which of the following is the MOST important consideration for effectively maintaining a risk register?

A. An IT owner is assigned for each risk scenario.
B. The register is updated frequently.
C. The register is shared with executive management.
D. Compensating controls are identified.

Answer: B

NEW QUESTION 4
- (Exam Topic 4)
During a risk assessment, a key external technology supplier refuses to provide control design and effectiveness information, citing confidentiality concerns. What should the risk practitioner do NEXT?

A. Escalate the non-cooperation to management
B. Exclude applicable controls from the assessment.
C. Review the supplier's contractual obligations.
D. Request risk acceptance from the business process owner.

Answer: C

NEW QUESTION 5
- (Exam Topic 4)
WhichT5f the following is the MOST effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage?

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

Answer: B

NEW QUESTION 6
- (Exam Topic 4)
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, program for all employees of the organization?

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

Answer: C

NEW QUESTION 7
- (Exam Topic 4)
Using key risk indicators (KRIs) to illustrate changes in the risk profile PRIMARILY helps to:

A. communicate risk trends to stakeholders.
B. assign ownership of emerging risk scenarios.
C. highlight noncompliance with the risk policy

D. identify threats to emerging technologies.

Answer: A

NEW QUESTION 8
- (Exam Topic 4)
When a risk practitioner is determining a system's criticality. it is MOST helpful to review the associated:

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

Answer: B

NEW QUESTION 9
- (Exam Topic 4)
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 4)
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 10
- (Exam Topic 4)
Which of the following is PRIMARILY a risk management responsibly of the first line of defense?

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

Answer: C

NEW QUESTION 14
- (Exam Topic 4)
An organization has decided to implement a new Internet of Things (loT) solution. Which of the following should be done FIRST when addressing security concerns associated with this new technology?

A. Develop new loT risk scenarios.
B. Implement loT device monitoring software.
C. Introduce controls to the new threat environment.
D. Engage external security reviews.

Answer: A

NEW QUESTION 18
- (Exam Topic 4)
A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

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

Answer: B

NEW QUESTION 21
- (Exam Topic 4)

After undertaking a risk assessment of a production system, the MOST appropriate action is fcr the risk manager to

A. recommend a program that minimizes the concerns of that production system.
B. inform the process owner of the concerns and propose measures to reduce them.
C. inform the IT manager of the concerns and propose measures to reduce them.
D. inform the development team of the concerns and together formulate risk reduction measures.

Answer: B

NEW QUESTION 23
- (Exam Topic 4)
An organization has decided to commit to a business activity with the knowledge that the risk exposure is higher than the risk appetite. Which of the following is the risk practitioner's MOST important action related to this decision?

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

Answer: C

NEW QUESTION 26
- (Exam Topic 4)
When establishing an enterprise IT risk management program, it is MOST important to:

A. review alignment with the organizations strategy.
B. understand the organization's information security policy.
C. validate the organization's data classification scheme.
D. report identified IT risk scenarios to senior management.

Answer: D

NEW QUESTION 27
- (Exam Topic 4)
An organization uses one centralized single sign-on (SSO) control to cover many applications. Which of the following is the BEST course of action when a new application is added to the environment after testing of the SSO control has been completed?

A. Initiate a retest of the full control
B. Retest the control using the new application as the only sample.
C. Review the corresponding change control documentation
D. Re-evaluate the control during (he next assessment

Answer: A

NEW QUESTION 32
- (Exam Topic 4)
Which of the following practices would be MOST effective in protecting personality identifiable information
(Ptl) from unauthorized access m a cloud environment?

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

Answer: B

NEW QUESTION 36
- (Exam Topic 4)
An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis Which of the following is the MOST important control to ensure the privacy of customer information?

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

Answer: C

NEW QUESTION 37
- (Exam Topic 4)
Which of the following is the MOST effective way to help ensure accountability for managing risk?

A. Assign process owners to key risk areas.
B. Obtain independent risk assessments.
C. Assign incident response action plan responsibilities.
D. Create accurate process narratives.

Answer: A

NEW QUESTION 41
- (Exam Topic 4)
A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?

A. Collaborate with the risk owner to determine the risk response plan.
B. Document the gap in the risk register and report to senior management.
C. Include a right to audit clause in the service provider contract.
D. Advise the risk owner to accept the risk.

Answer: C

NEW QUESTION 43
- (Exam Topic 4)
Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

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

Answer: A

NEW QUESTION 44
- (Exam Topic 4)
Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

A. Incomplete end-user device inventory
B. Unsupported end-user applications
C. Incompatible end-user devices
D. Multiple end-user device models

Answer: A

NEW QUESTION 45
- (Exam Topic 4)
Which of the following is the BEST method to maintain a common view of IT risk within an organization?

A. Collecting data for IT risk assessment
B. Establishing and communicating the IT risk profile
C. Utilizing a balanced scorecard
D. Performing and publishing an IT risk analysis

Answer: C

NEW QUESTION 48
- (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 49
- (Exam Topic 3)
The PRIMARY reason for prioritizing risk scenarios is to:

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

Answer: D

NEW QUESTION 51
- (Exam Topic 4)
A legacy application used for a critical business function relies on software that has reached the end of extended support Which of the following is the MOST effective control to manage this application?

A. Subscribe to threat intelligence to monitor external attacks.

B. Apply patches for a newer version of the application.
C. Segment the application within the existing network.
D. Increase the frequency of regular system and data backups.

Answer: D

NEW QUESTION 52
- (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 55
- (Exam Topic 3)
Which of the following should be considered when selecting a risk response?

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

Answer: B

NEW QUESTION 57
- (Exam Topic 3)
The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:

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

Answer: A

NEW QUESTION 62
- (Exam Topic 3)
An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

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

Answer: C

NEW QUESTION 64
- (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 67
- (Exam Topic 3)
Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

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

Answer: A

NEW QUESTION 72
- (Exam Topic 3)

The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:

A. changes due to emergencies.
B. changes that cause incidents.
C. changes not requiring user acceptance testing.
D. personnel that have rights to make changes in production.

Answer: B

NEW QUESTION 74
- (Exam Topic 3)
From a risk management perspective, the PRIMARY objective of using maturity models is to enable:

A. solution delivery.
B. resource utilization.
C. strategic alignment.
D. performance evaluation.

Answer: C

NEW QUESTION 79
- (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 80
- (Exam Topic 3)
An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?

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

Answer: D

NEW QUESTION 84
- (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 88
- (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 90
- (Exam Topic 3)
Which of the following is the PRIMARY risk management responsibility of the second line of defense?

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

Answer: A

NEW QUESTION 92
- (Exam Topic 3)
Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

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

Answer: C

NEW QUESTION 94
- (Exam Topic 3)
Which of the following is MOST important when developing key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 95
- (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 98
- (Exam Topic 3)
Which of the following should be the PRIMARY goal of developing information security metrics?

A. Raising security awareness
B. Enabling continuous improvement
C. Identifying security threats
D. Ensuring regulatory compliance

Answer: B

NEW QUESTION 102
- (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 103
- (Exam Topic 3)
Which of the following is the BEST evidence that a user account has been properly authorized?

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

Answer: C

NEW QUESTION 104
- (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 106
- (Exam Topic 3)
An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?

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

Answer: B

NEW QUESTION 108
- (Exam Topic 3)
Which of the following BEST indicates whether security awareness training is effective?

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

Answer: B

NEW QUESTION 111
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for risk related to IT infrastructure failure?

A. Number of times the recovery plan is reviewed
B. Number of successful recovery plan tests
C. Percentage of systems with outdated virus protection
D. Percentage of employees who can work remotely

Answer: B

NEW QUESTION 114
- (Exam Topic 3)
The PRIMARY reason to have risk owners assigned to entries in the risk register is to ensure:

A. risk is treated appropriately
B. mitigating actions are prioritized
C. risk entries are regularly updated
D. risk exposure is minimized.

Answer: A

NEW QUESTION 115
- (Exam Topic 3)
The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:

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

Answer: B

NEW QUESTION 116
- (Exam Topic 3)
When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs?

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

Answer: B

NEW QUESTION 120
- (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 122
- (Exam Topic 3)
Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:

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

Answer: D

NEW QUESTION 123
- (Exam Topic 3)
A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

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

Answer: D

NEW QUESTION 126
- (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 129
- (Exam Topic 3)
Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

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

Answer: A

NEW QUESTION 130
- (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 132
- (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 137
- (Exam Topic 3)
Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?

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

Answer: C

NEW QUESTION 141
- (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 142
- (Exam Topic 3)
Winch of the following key control indicators (KCIs) BEST indicates whether security requirements are identified and managed throughout a project He cycle?

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

Answer: A

NEW QUESTION 146
- (Exam Topic 3)
Which of the following would be MOST helpful to a risk practitioner when ensuring that mitigated risk remains within acceptable limits?

A. Building an organizational risk profile after updating the risk register
B. Ensuring risk owners participate in a periodic control testing process
C. Designing a process for risk owners to periodically review identified risk
D. Implementing a process for ongoing monitoring of control effectiveness

Answer: D

NEW QUESTION 150
- (Exam Topic 3)
Which of the following is the BEST way to mitigate the risk to IT infrastructure availability?

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

Answer: D

NEW QUESTION 153
- (Exam Topic 3)
Key risk indicators (KRIs) are MOST useful during which of the following risk management phases?

A. Monitoring
B. Analysis
C. Identification
D. Response selection

Answer: A

NEW QUESTION 157
- (Exam Topic 3)
Winch of the following is the BEST evidence of an effective risk treatment plan?

A. The inherent risk is below the asset residual risk.
B. Remediation cost is below the asset business value
C. The risk tolerance threshold s above the asset residual
D. Remediation is completed within the asset recovery time objective (RTO)

Answer: B

NEW QUESTION 162
- (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 165
- (Exam Topic 3)
When evaluating enterprise IT risk management it is MOST important to:

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

Answer: B

NEW QUESTION 166
- (Exam Topic 3)
Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

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

Answer: B

NEW QUESTION 168
- (Exam Topic 3)
Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

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

Answer: D

NEW QUESTION 171
- (Exam Topic 3)
What is the PRIMARY benefit of risk monitoring?

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

Answer: C

NEW QUESTION 176
- (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 181
- (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 184
- (Exam Topic 3)
Who should be accountable for monitoring the control environment to ensure controls are effective?

A. Risk owner
B. Security monitoring operations
C. Impacted data owner
D. System owner

Answer: A

NEW QUESTION 187
- (Exam Topic 3)
Which of the following BEST facilities the alignment of IT risk management with enterprise risk management (ERM)?

A. Adopting qualitative enterprise risk assessment methods
B. Linking IT risk scenarios to technology objectives
C. linking IT risk scenarios to enterprise strategy
D. Adopting quantitative enterprise risk assessment methods

Answer: C

NEW QUESTION 190
- (Exam Topic 3)
Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

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

Answer: A

NEW QUESTION 193
- (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 195
- (Exam Topic 3)
Which of the following approaches BEST identifies information systems control deficiencies?

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

Answer: C

NEW QUESTION 196
- (Exam Topic 3)
Which of the following would BEST indicate to senior management that IT processes are improving?

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

Answer: B

NEW QUESTION 200
- (Exam Topic 3)
Which of the following controls BEST enables an organization to ensure a complete and accurate IT asset inventory?

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

Answer: B

NEW QUESTION 202
- (Exam Topic 3)
Which of the following is the BEST way to quantify the likelihood of risk materialization?

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

Answer: D

NEW QUESTION 205
- (Exam Topic 3)
An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:

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

Answer: D

NEW QUESTION 208
- (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 212
- (Exam Topic 3)
A highly regulated organization acquired a medical technology startup company that processes sensitive personal information with weak data protection controls. Which of the following is the BEST way for the
acquiring company to reduce its risk while still enabling the flexibility needed by the startup company?

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

Answer: A

NEW QUESTION 216
- (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 218
- (Exam Topic 3)
Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

A. Compliance breaches are addressed in a timely manner.
B. Risk ownership is identified and assigned.
C. Risk treatment options receive adequate funding.
D. Residual risk is within risk tolerance.

Answer: B

NEW QUESTION 222
- (Exam Topic 3)
A deficient control has been identified which could result in great harm to an organization should a low frequency threat event occur. When communicating the associated risk to senior management the risk practitioner should explain:

A. mitigation plans for threat events should be prepared in the current planning period.
B. this risk scenario is equivalent to more frequent but lower impact risk scenarios.
C. the current level of risk is within tolerance.
D. an increase in threat events could cause a loss sooner than anticipated.

Answer: A

NEW QUESTION 224
- (Exam Topic 3)
All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

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

Answer: D

NEW QUESTION 225
- (Exam Topic 4)
Which of the following situations presents the GREATEST challenge to creating a comprehensive IT risk profile of an organization?

A. Manual vulnerability scanning processes
B. Organizational reliance on third-party service providers
C. Inaccurate documentation of enterprise architecture (EA)
D. Risk-averse organizational risk appetite

Answer: D

NEW QUESTION 226
- (Exam Topic 4)
Recovery the objectives (RTOs) should be based on

A. minimum tolerable downtime
B. minimum tolerable loss of data.
C. maximum tolerable downtime.
D. maximum tolerable loss of data

Answer: C

NEW QUESTION 228
- (Exam Topic 4)
Senior management is deciding whether to share confidential data with the organization's business partners. The BEST course of action for a risk practitioner would be to submit a report to senior management containing the:

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

Answer: A

NEW QUESTION 231
- (Exam Topic 4)
Which of the following is MOST helpful to understand the consequences of an IT risk event?

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

Answer: B

NEW QUESTION 232
- (Exam Topic 4)
Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?

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

Answer: C

NEW QUESTION 236

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

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

Answer: B

NEW QUESTION 237
- (Exam Topic 4)
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 241
- (Exam Topic 4)
Which of the following would BEST facilitate the implementation of data classification requirements?

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

Answer: B

NEW QUESTION 244
- (Exam Topic 4)
Which of the following activities BEST facilitates effective risk management throughout the organization?

A. Reviewing risk-related process documentation
B. Conducting periodic risk assessments
C. Performing a business impact analysis (BIA)
D. Performing frequent audits

Answer: B

NEW QUESTION 247
- (Exam Topic 4)
A recent vulnerability assessment of a web-facing application revealed several weaknesses. Which of the following should be done NEXT to determine the risk exposure?

A. Code review
B. Penetration test
C. Gap assessment
D. Business impact analysis (BIA)

Answer: B

NEW QUESTION 249
- (Exam Topic 4)
Which of the following would be a risk practitioner's BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

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

Answer: A

NEW QUESTION 254
- (Exam Topic 4)
Business management is seeking assurance from the CIO that IT has a plan in place for early identification of potential issues that could impact the delivery of a new application Which of the following is the BEST way to increase the chances of a successful delivery'?

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

Answer: D

NEW QUESTION 256
- (Exam Topic 4)
When implementing an IT risk management program, which of the following is the BEST time to evaluate current control effectiveness?

A. Before defining a framework
B. During the risk assessment
C. When evaluating risk response
D. When updating the risk register

Answer: B

NEW QUESTION 261
- (Exam Topic 4)
The PRIMARY objective of collecting information and reviewing documentation when performing periodic risk analysis should be to:

A. Identify new or emerging risk issues.
B. Satisfy audit requirements.
C. Survey and analyze historical risk data.
D. Understand internal and external threat agents.

Answer: D

NEW QUESTION 265
- (Exam Topic 4)
An organization's chief information officer (CIO) has proposed investing in a new. untested technology to take advantage of being first to market Senior management has concerns about the success of the project and has set a limit for expenditures before final approval. This conditional approval indicates the organization's risk:

A. capacity.
B. appetite.
C. management capability.
D. treatment strategy.

Answer: B

NEW QUESTION 267
- (Exam Topic 4)
Which of the following contributes MOST to the effective implementation of risk responses?

A. Clear understanding of the risk
B. Comparable industry risk trends
C. Appropriate resources
D. Detailed standards and procedures

Answer: A

NEW QUESTION 271
- (Exam Topic 4)
A zero-day vulnerability has been discovered in a globally used brand of hardware server that allows hackers to gain access to affected IT systems. Which of the following is MOST likely to change as a result of this situation?

A. Control effectiveness
B. Risk appetite
C. Risk likelihood
D. Key risk indicator (KRI)

Answer: C

NEW QUESTION 276
- (Exam Topic 4)
When preparing a risk status report for periodic review by senior management, it is MOST important to ensure the report includes

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

Answer: A

NEW QUESTION 278
- (Exam Topic 4)
The BEST indicator of the risk appetite of an organization is the

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

Answer: B

NEW QUESTION 281
- (Exam Topic 4)
Which of the following would MOST likely require a risk practitioner to update the risk register?

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

Answer: C

NEW QUESTION 286
- (Exam Topic 4)
Who is BEST suited to provide objective input when updating residual risk to reflect the results of control effectiveness?

A. Control owner
B. Risk owner
C. Internal auditor
D. Compliance manager

Answer: C

NEW QUESTION 287
- (Exam Topic 4)
Which of the following is the BEST recommendation to address recent IT risk trends that indicate social
engineering attempts are increasing in the organization?

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

Answer: A

NEW QUESTION 292
- (Exam Topic 4)
Which of the following s MOST likely to deter an employee from engaging in inappropriate use of company owned IT systems?

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

Answer: D

NEW QUESTION 296
- (Exam Topic 4)
Who is MOST appropriate to be assigned ownership of a control

A. The individual responsible for control operation
B. The individual informed of the control effectiveness
C. The individual responsible for resting the control
D. The individual accountable for monitoring control effectiveness

Answer: D

NEW QUESTION 299
- (Exam Topic 4)
A control process has been implemented in response to a new regulatory requirement, but has significantly reduced productivity. Which of the following is the
BEST way to resolve this concern?

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

Answer: C

NEW QUESTION 303

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

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

Answer: C

NEW QUESTION 307
- (Exam Topic 4)
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 312
- (Exam Topic 4)
Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

A. The number of stakeholders involved in IT risk identification workshops
B. The percentage of corporate budget allocated to IT risk activities
C. The percentage of incidents presented to the board
D. The number of executives attending IT security awareness training

Answer: B

NEW QUESTION 313
- (Exam Topic 4)
Which of the following is the GREATEST benefit of centralizing IT systems?

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

Answer: C

NEW QUESTION 315
- (Exam Topic 4)
An organization has experienced several incidents of extended network outages that have exceeded tolerance. Which of the following should be the risk practitioner's FIRST step to address this situation?

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

Answer: D

NEW QUESTION 319
- (Exam Topic 4)
Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

A. The report was provided directly from the vendor.
B. The risk associated with multiple control gaps was accepted.
C. The control owners disagreed with the auditor's recommendations.
D. The controls had recurring noncompliance.

Answer: A

NEW QUESTION 320
- (Exam Topic 4)
Which of the following is MOST important to promoting a risk-aware culture?

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

Answer: D

NEW QUESTION 321
- (Exam Topic 4)
The MAJOR reason to classify information assets is

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

Answer: C

NEW QUESTION 322
- (Exam Topic 4)
Which of the following is the PRIMARY objective of maintaining an information asset inventory?

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

Answer: B

NEW QUESTION 324
- (Exam Topic 4)
Which of the following is MOST helpful in providing an overview of an organization's risk management program?

A. Risk management treatment plan
B. Risk assessment results
C. Risk management framework
D. Risk register

Answer: C

NEW QUESTION 328
- (Exam Topic 4)
Which of the following BEST reduces the risk associated with the theft of a laptop containing sensitive information?

A. Cable lock
B. Data encryption
C. Periodic backup
D. Biometrics access control

Answer: B

NEW QUESTION 333
- (Exam Topic 4)
Which of the following is the BEST approach for selecting controls to minimize risk?

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

Answer: C

NEW QUESTION 336
- (Exam Topic 4)
Which of the following proposed benefits is MOST likely to influence senior management approval to reallocate budget for a new security initiative?

A. Reduction in the number of incidents
B. Reduction in inherent risk
C. Reduction in residual risk
D. Reduction in the number of known vulnerabilities

Answer: B

NEW QUESTION 341
- (Exam Topic 4)
Which of the following is the BEST way to protect sensitive data from administrators within a public cloud?

A. Use an encrypted tunnel lo connect to the cloud.
B. Encrypt the data in the cloud database.
C. Encrypt physical hard drives within the cloud.

D. Encrypt data before it leaves the organization.

Answer: D

NEW QUESTION 344
- (Exam Topic 4)
Which of the following provides the MOST reliable evidence of a control's effectiveness?

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

Answer: D

NEW QUESTION 348
- (Exam Topic 4)
Which of the following is the BEST course of action when an organization wants to reduce likelihood in order to reduce a risk level?

A. Monitor risk controls.
B. Implement preventive measures.
C. Implement detective controls.
D. Transfer the risk.

Answer: B

NEW QUESTION 349
- (Exam Topic 4)
An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

A. Limited organizational knowledge of the underlying technology
B. Lack of commercial software support
C. Varying costs related to implementation and maintenance
D. Slow adoption of the technology across the financial industry

Answer: A

NEW QUESTION 352
- (Exam Topic 4)
Which of the following is the result of a realized risk scenario?

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

Answer: D

NEW QUESTION 355
- (Exam Topic 4)
Which of the following is MOST important for senior management to review during an acquisition?

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

Answer: A

NEW QUESTION 357
- (Exam Topic 4)
Which of the following is MOST important to update when an organization's risk appetite changes?

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

Answer: A

NEW QUESTION 362
- (Exam Topic 4)
Which of the following would be the GREATEST concern for an IT risk practitioner when an employees.....

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

Answer: B

NEW QUESTION 365
- (Exam Topic 4)
What is the BEST recommendation to reduce the risk associated with potential system compromise when a vendor stops releasing security patches and updates for a business-critical legacy system?

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

Answer: A

NEW QUESTION 370
- (Exam Topic 4)
Who is the BEST person to the employee personal data?

A. Human resources (HR) manager
B. System administrator
C. Data privacy manager
D. Compliance manager

Answer: A

NEW QUESTION 374
- (Exam Topic 4)
Which of the following should be accountable for ensuring that media containing financial information are adequately destroyed per an organization's data disposal policy?

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

Answer: C

NEW QUESTION 379
- (Exam Topic 4)
An IT risk threat analysis is BEST used to establish

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

Answer: A

NEW QUESTION 382
- (Exam Topic 4)
It is MOST important that security controls for a new system be documented in:

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

Answer: C

NEW QUESTION 384
- (Exam Topic 4)
Which of the following is the GREATEST benefit of identifying appropriate risk owners?

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

Answer: A

NEW QUESTION 388

- (Exam Topic 4)
Which of the following is the GREATEST concern when establishing key risk indicators (KRIs)?

A. High percentage of lagging indicators
B. Nonexistent benchmark analysis
C. Incomplete documentation for KRI monitoring
D. Ineffective methods to assess risk

Answer: B

NEW QUESTION 389
- (Exam Topic 4)
Which organization is implementing a project to automate the purchasing process, including the modification of approval controls. Which of the following tasks is lie responsibility of the risk practitioner*?

A. Verify that existing controls continue to properly mitigate defined risk
B. Test approval process controls once the project is completed
C. Update the existing controls for changes in approval processes from this project
D. Perform a gap analysis of the impacted control processes

Answer: B

NEW QUESTION 390
- (Exam Topic 4)
Which of the following is MOST important to determine as a result of a risk assessment?

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

Answer: D

NEW QUESTION 393
- (Exam Topic 4)
The MAIN purpose of selecting a risk response is to.

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

Answer: C

NEW QUESTION 394
- (Exam Topic 4)
During a risk assessment, a risk practitioner learns that an IT risk factor is adequately mitigated by compensating controls in an associated business process. Which of the following would enable the MOST effective management of the residual risk?

A. Schedule periodic reviews of the compensating controls' effectiveness.
B. Report the use of compensating controls to senior management.
C. Recommend additional IT controls to further reduce residual risk.
D. Request that ownership of the compensating controls is reassigned to IT

Answer: A

NEW QUESTION 397
- (Exam Topic 4)
An internal audit report reveals that a legacy system is no longer supported Which of the following is the risk practitioner's MOST important action before recommending a risk response'

A. Review historical application down me and frequency
B. Assess the potential impact and cost of mitigation
C. identify other legacy systems within the organization
D. Explore the feasibility of replacing the legacy system

Answer: B

NEW QUESTION 398
- (Exam Topic 4)
Which of the following is a risk practitioner's BEST course of action after identifying risk scenarios related to noncompliance with new industry regulations?

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

Answer: D

NEW QUESTION 401
- (Exam Topic 3)
Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

A. Activity logging and monitoring
B. Periodic access review
C. Two-factor authentication
D. Awareness training and background checks

Answer: A

NEW QUESTION 405
- (Exam Topic 3)
Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

A. Senior management has approved the control design.
B. Inherent risk has been reduced from original levels.
C. Residual risk remains within acceptable levels.
D. Costs for control maintenance are reasonable.

Answer: C

NEW QUESTION 406
- (Exam Topic 3)
To minimize the risk of a potential acquisition being exposed externally, an organization has selected a few
key employees to be engaged in the due diligence process. A member of the due diligence team realizes a close acquaintance is a high-ranking IT professional at
a subsidiary of the company about to be acquired. What is the BEST course of action for this team member?

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

Answer: B

NEW QUESTION 409
- (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 410
- (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 413
- (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 418
- (Exam Topic 3)
Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

A. Updating the risk register to include the risk mitigation plan
B. Determining processes for monitoring the effectiveness of the controls
C. Ensuring that control design reduces risk to an acceptable level
D. Confirming to management the controls reduce the likelihood of the risk

Answer: C

NEW QUESTION 423
- (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 427
- (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 432
- (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 436
- (Exam Topic 3)
Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

A. Organizational reporting process
B. Incident reporting procedures
C. Regularly scheduled audits
D. Incident management policy

Answer: A

NEW QUESTION 437
- (Exam Topic 3)
Which of the following would be the GREATEST challenge when implementing a corporate risk framework for a global organization?

A. Privacy risk controls
B. Business continuity
C. Risk taxonomy
D. Management support

Answer: A

NEW QUESTION 442
- (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 446
- (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 450
- (Exam Topic 3)
The acceptance of control costs that exceed risk exposure MOST likely demonstrates:

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

Answer: C

NEW QUESTION 451
- (Exam Topic 3)
Which of the following is MOST important when developing risk scenarios?

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

Answer: D

NEW QUESTION 453
- (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 456
- (Exam Topic 3)
Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?

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

Answer: A

NEW QUESTION 459
- (Exam Topic 3)
Which of the following is a drawback in the use of quantitative risk analysis?

A. It assigns numeric values to exposures of assets.
B. It requires more resources than other methods
C. It produces the results in numeric form.
D. It is based on impact analysis of information assets.

Answer: B

NEW QUESTION 464
- (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 467
- (Exam Topic 3)
Which of the following would provide the MOST useful information to a risk owner when reviewing the progress of risk mitigation?

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

Answer: C

NEW QUESTION 472
- (Exam Topic 3)
A risk practitioner has become aware of production data being used in a test environment. Which of the following should be the practitioner's PRIMARY concern?

A. Sensitivity of the data
B. Readability of test data
C. Security of the test environment
D. Availability of data to authorized staff

Answer: A

NEW QUESTION 476
- (Exam Topic 3)
The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

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

Answer: D

NEW QUESTION 478
- (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 479
- (Exam Topic 3)
An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

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

Answer: B

NEW QUESTION 484
- (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 486
- (Exam Topic 3)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an antivirus program?

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

Answer: A

NEW QUESTION 489
- (Exam Topic 3)
An organization is implementing encryption for data at rest to reduce the risk associated with unauthorized access. Which of the following MUST be considered to assess the residual risk?

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

Answer: D

NEW QUESTION 490
- (Exam Topic 3)
When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction
based on:

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

Answer: A

NEW QUESTION 494
- (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 497
- (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 498
- (Exam Topic 3)
Which of the following is the FIRST step when conducting a business impact analysis (BIA)?

A. Identifying critical information assets
B. Identifying events impacting continuity of operations;
C. Creating a data classification scheme
D. Analyzing previous risk assessment results

Answer: A

NEW QUESTION 502
- (Exam Topic 3)

An organization practices the principle of least privilege. To ensure access remains appropriate, application owners should be required to review user access rights on a regular basis by obtaining:

A. business purpose documentation and software license counts
B. an access control matrix and approval from the user's manager
C. documentation indicating the intended users of the application
D. security logs to determine the cause of invalid login attempts

Answer: B

NEW QUESTION 507
- (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 511
- (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 514
- (Exam Topic 3)
Which of the following provides the MOST useful information when developing a risk profile for management approval?

A. Residual risk and risk appetite
B. Strength of detective and preventative controls
C. Effectiveness and efficiency of controls
D. Inherent risk and risk tolerance

Answer: A

NEW QUESTION 519
- (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 522
- (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 525
- (Exam Topic 2)
A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner's FIRST course of action?

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

Answer: D

NEW QUESTION 528
- (Exam Topic 2)
Controls should be defined during the design phase of system development because:

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

Answer: A

NEW QUESTION 532
- (Exam Topic 2)
Which of the following BEST measures the efficiency of an incident response process?

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

Answer: C

NEW QUESTION 533
- (Exam Topic 2)
IT disaster recovery point objectives (RPOs) should be based on the:

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

Answer: C

NEW QUESTION 538
- (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 543
- (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 547
- (Exam Topic 2)
Which of the following key risk indicators (KRIs) is MOST effective for monitoring risk related to a bring your own device (BYOD) program?

A. Number of users who have signed a BYOD acceptable use policy
B. Number of incidents originating from BYOD devices
C. Budget allocated to the BYOD program security controls
D. Number of devices enrolled in the BYOD program

Answer: D

NEW QUESTION 551
- (Exam Topic 2)
Which of The following is the MOST relevant information to include in a risk management strategy?

A. Quantified risk triggers
B. Cost of controls
C. Regulatory requirements

D. Organizational goals

Answer: D

NEW QUESTION 552
- (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 553
- (Exam Topic 2)
An organization has granted a vendor access to its data in order to analyze customer behavior. Which of the following would be the MOST effective control to mitigate the risk of customer data leakage?

A. Enforce criminal background checks.
B. Mask customer data fields.
C. Require vendor to sign a confidentiality agreement.
D. Restrict access to customer data on a "need to know" basis.

Answer: D

NEW QUESTION 556
- (Exam Topic 2)
Who should be responsible for strategic decisions on risk management?

A. Chief information officer (CIO)
B. Executive management team
C. Audit committee
D. Business process owner

Answer: B

NEW QUESTION 560
- (Exam Topic 2)
The PRIMARY basis for selecting a security control is:

A. to achieve the desired level of maturity.
B. the materiality of the risk.
C. the ability to mitigate risk.
D. the cost of the control.

Answer: C

NEW QUESTION 563
- (Exam Topic 2)
Which of the following is the BEST way to detect zero-day malware on an end user's workstation?

A. An antivirus program
B. Database activity monitoring
C. Firewall log monitoring
D. File integrity monitoring

Answer: C

NEW QUESTION 568
- (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 570
- (Exam Topic 2)
Which of the following conditions presents the GREATEST risk to an application?

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

Answer: D

NEW QUESTION 571
- (Exam Topic 2)
What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

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

Answer: B

NEW QUESTION 572
- (Exam Topic 2)
Due to a change in business processes, an identified risk scenario no longer requires mitigation. Which of the following is the MOST important reason the risk should remain in the risk register?

A. To support regulatory requirements
B. To prevent the risk scenario in the current environment
C. To monitor for potential changes to the risk scenario
D. To track historical risk assessment results

Answer: C

NEW QUESTION 575
- (Exam Topic 2)
An IT organization is replacing the customer relationship management (CRM) system. Who should own the risk associated with customer data leakage caused by insufficient IT security controls for the new system?

A. Chief information security officer
B. Business process owner
C. Chief risk officer
D. IT controls manager

Answer: B

NEW QUESTION 580
- (Exam Topic 2)
An organization is considering modifying its system to enable acceptance of credit card payments. To reduce the risk of data exposure, which of the following should the organization do FIRST?

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

Answer: A

NEW QUESTION 581
- (Exam Topic 2)
Which of the following is the PRIMARY reason to establish the root cause of an IT security incident?

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

Answer: D

NEW QUESTION 584
- (Exam Topic 2)
Deviation from a mitigation action plan's completion date should be determined by which of the following?

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

Answer: D

NEW QUESTION 588
- (Exam Topic 2)
The BEST key performance indicator (KPI) to measure the effectiveness of a vendor risk management program is the percentage of:

A. vendors providing risk assessments on time.
B. vendor contracts reviewed in the past year.
C. vendor risk mitigation action items completed on time.
D. vendors that have reported control-related incidents.

Answer: A

NEW QUESTION 591
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to ensure once a risk action plan has been completed?

A. The risk owner has validated outcomes.
B. The risk register has been updated.
C. The control objectives are mapped to risk objectives.
D. The requirements have been achieved.

Answer: B

NEW QUESTION 593
- (Exam Topic 2)
Which of the following should be the PRIMARY focus of an independent review of a risk management process?

A. Accuracy of risk tolerance levels
B. Consistency of risk process results
C. Participation of stakeholders
D. Maturity of the process

Answer: B

NEW QUESTION 597
- (Exam Topic 2)
The BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability remediation program is the number of:

A. vulnerability scans.
B. recurring vulnerabilities.
C. vulnerabilities remediated,
D. new vulnerabilities identified.

Answer: C

NEW QUESTION 602
- (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 607
- (Exam Topic 2)
Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

A. An internal audit
B. Security operations center review
C. Internal penetration testing
D. A third-party audit

Answer: D

NEW QUESTION 612
- (Exam Topic 2)
An organization's risk tolerance should be defined and approved by which of the following?

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

Answer: B

NEW QUESTION 615
- (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 620
- (Exam Topic 2)
An IT risk practitioner is evaluating an organization's change management controls over the last six months. The GREATEST concern would be an increase in:

A. rolled back changes below management's thresholds.
B. change-related exceptions per month.
C. the average implementation time for changes.
D. number of user stories approved for implementation.

Answer: B

NEW QUESTION 625
- (Exam Topic 2)
Which of the following should be the PRIMARY objective of a risk awareness training program?

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

Answer: A

NEW QUESTION 628
- (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 630
- (Exam Topic 2)
Reviewing which of the following provides the BEST indication of an organizations risk tolerance?

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

Answer: D

NEW QUESTION 635
- (Exam Topic 2)
Which of the following can be used to assign a monetary value to risk?

A. Annual loss expectancy (ALE)
B. Business impact analysis
C. Cost-benefit analysis
D. Inherent vulnerabilities

Answer: A

NEW QUESTION 639
- (Exam Topic 2)
The risk associated with a high-risk vulnerability in an application is owned by the:

A. security department.
B. business unit
C. vendor.
D. IT department.

Answer:

B

NEW QUESTION 640
- (Exam Topic 2)
Which of the following is the MOST important consideration when determining whether to accept residual risk after security controls have been implemented on a critical system?

A. Cost versus benefit of additional mitigating controls
B. Annualized loss expectancy (ALE) for the system
C. Frequency of business impact
D. Cost of the Information control system

Answer: A

NEW QUESTION 644
- (Exam Topic 2)
A risk practitioner has observed that risk owners have approved a high number of exceptions to the information security policy. Which of the following should be the risk practitioner's GREATEST concern?

A. Security policies are being reviewed infrequently.
B. Controls are not operating efficiently.
C. Vulnerabilities are not being mitigated
D. Aggregate risk is approaching the tolerance threshold

Answer: D

NEW QUESTION 645
- (Exam Topic 2)
Who is responsible for IT security controls that are outsourced to an external service provider?

A. Organization's information security manager
B. Organization's risk function
C. Service provider's IT management
D. Service provider's information security manager

Answer: B

NEW QUESTION 647
- (Exam Topic 2)
Following a significant change to a business process, a risk practitioner believes the associated risk has been reduced. The risk practitioner should advise the risk owner to FIRST

A. review the key risk indicators.
B. conduct a risk analysis.
C. update the risk register
D. reallocate risk response resources.

Answer: A

NEW QUESTION 650
- (Exam Topic 2)
Which of the following is the MOST important consideration when performing a risk assessment of a fire suppression system within a data center?

A. Insurance coverage
B. Onsite replacement availability
C. Maintenance procedures
D. Installation manuals

Answer: C

NEW QUESTION 652
- (Exam Topic 2)
A risk assessment indicates the residual risk associated with a new bring your own device (BYOD) program is within organizational risk tolerance. Which of the following should the risk practitioner
recommend be done NEXT?

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

Answer: B

NEW QUESTION 653
- (Exam Topic 2)
To minimize risk in a software development project, when is the BEST time to conduct a risk analysis?

A. During the business requirement definitions phase
B. Before periodic steering committee meetings
C. At each stage of the development life cycle
D. During the business case development

Answer: A

NEW QUESTION 654
- (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 659
- (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 664
- (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 665
- (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 666
- (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 671
- (Exam Topic 2)
A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

A. Determine changes in the risk level.
B. Outsource the vulnerability management process.
C. Review the patch management process.
D. Add agenda item to the next risk committee meeting.

Answer: C

NEW QUESTION 676

- (Exam Topic 2)
Business areas within an organization have engaged various cloud service providers directly without assistance from the IT department. What should the risk practitioner do?

A. Recommend the IT department remove access to the cloud services.
B. Engage with the business area managers to review controls applied.
C. Escalate to the risk committee.
D. Recommend a risk assessment be conducted.

Answer: B

NEW QUESTION 679
- (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 684
- (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 689
- (Exam Topic 2)
A business unit has decided to accept the risk of implementing an off-the-shelf, commercial software package that uses weak password controls. The BEST course of action would be to:

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

Answer: B

NEW QUESTION 694
- (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 698
- (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 701
- (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 706
- (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 710
- (Exam Topic 2)
A bank has outsourced its statement printing function to an external service provider. Which of the following is the MOST critical requirement to include in the contract?

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

Answer: D

NEW QUESTION 715
- (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 718
- (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 723
- (Exam Topic 2)
Who should be responsible for implementing and maintaining security controls?

A. End user
B. Internal auditor
C. Data owner
D. Data custodian

Answer: C

NEW QUESTION 727
- (Exam Topic 2)
Which of the following methods would BEST contribute to identifying obscure risk scenarios?

A. Brainstorming sessions
B. Control self-assessments
C. Vulnerability analysis
D. Monte Carlo analysis

Answer: A

NEW QUESTION 730
- (Exam Topic 2)
An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

A. Number of customer records held
B. Number of databases that host customer data
C. Number of encrypted customer databases
D. Number of staff members having access to customer data

Answer: B

NEW QUESTION 735
- (Exam Topic 2)
A risk practitioner has been notified that an employee sent an email in error containing customers' personally identifiable information (PII). Which of the following is the risk practitioner's BEST course of action?

A. Report it to the chief risk officer.
B. Advise the employee to forward the email to the phishing team.
C. follow incident reporting procedures.
D. Advise the employee to permanently delete the email.

Answer: C

NEW QUESTION 740
- (Exam Topic 2)
What is MOST important for the risk practitioner to understand when creating an initial IT risk register?

A. Enterprise architecture (EA)
B. Control environment
C. IT objectives
D. Organizational objectives

Answer: D

NEW QUESTION 742
- (Exam Topic 2)
The PRIMARY goal of a risk management program is to:

A. facilitate resource availability.
B. help ensure objectives are met.
C. safeguard corporate assets.
D. help prevent operational losses.

Answer: D

NEW QUESTION 743
- (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 748
- (Exam Topic 2)
Which of the following is MOST important to the effective monitoring of key risk indicators (KRIS)?

A. Updating the threat inventory with new threats
B. Automating log data analysis
C. Preventing the generation of false alerts
D. Determining threshold levels

Answer: D

NEW QUESTION 753
- (Exam Topic 2)
Which of the following BEST helps to identify significant events that could impact an organization? Vulnerability analysis

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

Answer: C

NEW QUESTION 758
- (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 763
- (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 768
- (Exam Topic 2)
Which of the following is a risk practitioner's BEST course of action upon learning that a control under internal review may no longer be necessary?

A. Obtain approval to retire the control.
B. Update the status of the control as obsolete.
C. Consult the internal auditor for a second opinion.
D. Verify the effectiveness of the original mitigation plan.

Answer: B

NEW QUESTION 772
- (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 776
- (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 780
- (Exam Topic 2)
Which of the following is the PRIMARY reason to update a risk register with risk assessment results?

A. To communicate the level and priority of assessed risk to management
B. To provide a comprehensive inventory of risk across the organization
C. To assign a risk owner to manage the risk
D. To enable the creation of action plans to address nsk

Answer: A

NEW QUESTION 783
- (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 787

- (Exam Topic 2)
Which of the following would MOST likely drive the need to review and update key performance indicators (KPIs) for critical IT assets?

A. The outsourcing of related IT processes
B. Outcomes of periodic risk assessments
C. Changes in service level objectives
D. Findings from continuous monitoring

Answer: B

NEW QUESTION 788
- (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 793
- (Exam Topic 2)
Which of the following is the PRIMARY reason for conducting peer reviews of risk analysis?

A. To enhance compliance with standards
B. To minimize subjectivity of assessments
C. To increase consensus among peers
D. To provide assessments for benchmarking

Answer: B

NEW QUESTION 794
- (Exam Topic 2)
The implementation of a risk treatment plan will exceed the resources originally allocated for the risk response. Which of the following should be the risk owner's NEXT action?

A. Perform a risk assessment.
B. Accept the risk of not implementing.
C. Escalate to senior management.
D. Update the implementation plan.

Answer: C

NEW QUESTION 798
- (Exam Topic 2)
A software developer has administrative access to a production application. Which of the following should be of GREATEST concern to a risk practitioner?

A. The administrative access does not allow for activity log monitoring.
B. The administrative access does not follow password management protocols.
C. The administrative access represents a deviation from corporate policy.
D. The administrative access represents a segregation of duties conflict.

Answer: D

NEW QUESTION 803
- (Exam Topic 2)
An organization has identified that terminated employee accounts are not disabled or deleted within the time required by corporate policy. Unsure of the reason, the organization has decided to monitor the situation for three months to obtain more information. As a result of this decision, the risk has been:

A. avoided.
B. accepted.
C. mitigated.
D. transferred.

Answer: B

NEW QUESTION 807
- (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 812
- (Exam Topic 2)
When presenting risk, the BEST method to ensure that the risk is measurable against the organization's risk appetite is through the use of a:

A. risk map
B. cause-and-effect diagram
C. maturity model
D. technology strategy plan.

Answer: C

NEW QUESTION 816
- (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 820
- (Exam Topic 2)
Which of the following is the MOST important enabler of effective risk management?

A. User awareness of policies and procedures
B. Implementation of proper controls
C. Senior management support
D. Continuous monitoring of threats and vulnerabilities

Answer: C

NEW QUESTION 825
- (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 827
- (Exam Topic 2)
Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?

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

Answer: A

NEW QUESTION 830
- (Exam Topic 2)
Which of the following presents the GREATEST challenge for an IT risk practitioner who wants to report on trends in historical IT risk levels?

A. Qualitative measures for potential loss events
B. Changes in owners for identified IT risk scenarios
C. Changes in methods used to calculate probability
D. Frequent use of risk acceptance as a treatment option

Answer: A

NEW QUESTION 831
- (Exam Topic 2)
Once a risk owner has decided to implement a control to mitigate risk, it is MOST important to develop:

A. a process for measuring and reporting control performance.
B. an alternate control design in case of failure of the identified control.
C. a process for bypassing control procedures in case of exceptions.
D. procedures to ensure the effectiveness of the control.

Answer: A

NEW QUESTION 836
- (Exam Topic 2)
Which of the following provides The BEST information when determining whether to accept residual risk of a critical system to be implemented?

A. Single loss expectancy (SLE)
B. Cost of the information system
C. Availability of additional compensating controls
D. Potential business impacts are within acceptable levels

Answer: D

NEW QUESTION 838
- (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 840
- (Exam Topic 2)
A large organization needs to report risk at all levels for a new centralized visualization project to reduce cost and improve performance. Which of the following would MOST effectively represent the overall risk of the project to senior management?

A. Aggregated key performance indicators (KPIs)
B. Key risk indicators (KRIs)
C. Centralized risk register
D. Risk heat map

Answer: D

NEW QUESTION 842
- (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 847
- (Exam Topic 2)
A monthly payment report is generated from the enterprise resource planning (ERP) software to validate data against the old and new payroll systems. What is the BEST way to mitigate the risk associated with data integrity loss in the new payroll system after data migration?

A. Compare new system reports with functional requirements.
B. Compare encrypted data with checksums.
C. Compare results of user acceptance testing (UAT) with the testing criteria.
D. Compare processing output from both systems using the previous month's data.

Answer: D

NEW QUESTION 850
- (Exam Topic 1)
Which of the following is the PRIMARY reason for a risk practitioner to use global standards related to risk management?

A. To build an organizational risk-aware culture
B. To continuously improve risk management processes
C. To comply with legal and regulatory requirements
D. To identify gaps in risk management practices

Answer: B

NEW QUESTION 854
- (Exam Topic 2)
Which of the following is the GREATEST concern associated with the transmission of healthcare data across the internet?

A. Unencrypted data
B. Lack of redundant circuits
C. Low bandwidth connections
D. Data integrity

Answer: A

NEW QUESTION 859
- (Exam Topic 1)
Which of the following is the MOST important foundational element of an effective three lines of defense model for an organization?

A. A robust risk aggregation tool set
B. Clearly defined roles and responsibilities
C. A well-established risk management committee
D. Well-documented and communicated escalation procedures

Answer: B

NEW QUESTION 860
- (Exam Topic 1)
Which of the following is the FIRST step in managing the security risk associated with wearable technology in the workplace?

A. Identify the potential risk.
B. Monitor employee usage.
C. Assess the potential risk.
D. Develop risk awareness training.

Answer: A

NEW QUESTION 861
- (Exam Topic 1)
Which of the following BEST provides an early warning that network access of terminated employees is not being revoked in accordance with the service level agreement (SLA)?

A. Updating multi-factor authentication
B. Monitoring key access control performance indicators
C. Analyzing access control logs for suspicious activity
D. Revising the service level agreement (SLA)

Answer: B

NEW QUESTION 863
- (Exam Topic 1)
A global organization is considering the acquisition of a competitor. Senior management has requested a review of the overall risk profile from the targeted organization. Which of the following components of this review would provide the MOST useful information?

A. Risk appetite statement
B. Enterprise risk management framework
C. Risk management policies
D. Risk register

Answer: D

NEW QUESTION 864
- (Exam Topic 1)
A contract associated with a cloud service provider MUST include:

A. ownership of responsibilities.
B. a business recovery plan.
C. provision for source code escrow.
D. the providers financial statements.

Answer: A

NEW QUESTION 865
- (Exam Topic 1)
Which of the following is the BEST way for a risk practitioner to help management prioritize risk response?

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

Answer: B

NEW QUESTION 868

- (Exam Topic 1)
The number of tickets to rework application code has significantly exceeded the established threshold. Which of the following would be the risk practitioner s BEST recommendation?

A. Perform a root cause analysis
B. Perform a code review
C. Implement version control software.
D. Implement training on coding best practices

Answer: A

NEW QUESTION 871
- (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 876
- (Exam Topic 1)
During the risk assessment of an organization that processes credit cards, a number of existing controls have been found to be ineffective and do not meet industry standards. The overall control environment may still be effective if:

A. compensating controls are in place.
B. a control mitigation plan is in place.
C. risk management is effective.
D. residual risk is accepted.

Answer: A

NEW QUESTION 877
- (Exam Topic 1)
Who should be accountable for ensuring effective cybersecurity controls are established?

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

Answer: B

NEW QUESTION 882
- (Exam Topic 1)
IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would be MOST helpful?

A. IT risk register
B. List of key risk indicators
C. Internal audit reports
D. List of approved projects

Answer: A

NEW QUESTION 883
- (Exam Topic 1)
An organization has identified a risk exposure due to weak technical controls in a newly implemented HR system. The risk practitioner is documenting the risk in the risk register. The risk should be owned by the:

A. chief risk officer.
B. project manager.
C. chief information officer.
D. business process owner.

Answer: D

NEW QUESTION 885
- (Exam Topic 1)
Which of the following would MOST effectively enable a business operations manager to identify events exceeding risk thresholds?

A. Continuous monitoring
B. A control self-assessment
C. Transaction logging
D. Benchmarking against peers

Answer: A

NEW QUESTION 889
- (Exam Topic 1)
A risk assessment has identified that an organization may not be in compliance with industry regulations. The BEST course of action would be to:

A. conduct a gap analysis against compliance criteria.
B. identify necessary controls to ensure compliance.
C. modify internal assurance activities to include control validation.
D. collaborate with management to meet compliance requirements.

Answer: A

NEW QUESTION 893
- (Exam Topic 1)
Which of the following is the MOST important factor affecting risk management in an organization?

A. The risk manager's expertise
B. Regulatory requirements
C. Board of directors' expertise
D. The organization's culture

Answer: D

NEW QUESTION 897
- (Exam Topic 1)
Which of the following is the MOST important data source for monitoring key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 902
- (Exam Topic 1)
Whether the results of risk analyses should be presented in quantitative or qualitative terms should be based PRIMARILY on the:

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

Answer: A

NEW QUESTION 903
- (Exam Topic 1)
Which of the following should be the PRIMARY input when designing IT controls?

A. Benchmark of industry standards
B. Internal and external risk reports
C. Recommendations from IT risk experts
D. Outcome of control self-assessments

Answer: B

NEW QUESTION 905
- (Exam Topic 1)
A business unit is updating a risk register with assessment results for a key project. Which of the following is MOST important to capture in the register?

A. The team that performed the risk assessment
B. An assigned risk manager to provide oversight
C. Action plans to address risk scenarios requiring treatment
D. The methodology used to perform the risk assessment

Answer: B

NEW QUESTION 909
- (Exam Topic 1)
Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?

A. Assess the vulnerability management process.
B. Conduct a control serf-assessment.

C. Conduct a vulnerability assessment.
D. Reassess the inherent risk of the target.

Answer: A

NEW QUESTION 912
- (Exam Topic 1)
The PRIMARY advantage of implementing an IT risk management framework is the:

A. establishment of a reliable basis for risk-aware decision making.
B. compliance with relevant legal and regulatory requirements.
C. improvement of controls within the organization and minimized losses.
D. alignment of business goals with IT objectives.

Answer: A

NEW QUESTION 915
- (Exam Topic 1)
An organization has allowed its cyber risk insurance to lapse while seeking a new insurance provider. The risk practitioner should report to management that the risk has been:

A. transferred
B. mitigated.
C. accepted
D. avoided

Answer: C

NEW QUESTION 917
- (Exam Topic 1)
Which of the following would BEST help to ensure that suspicious network activity is identified?

A. Analyzing intrusion detection system (IDS) logs
B. Analyzing server logs
C. Using a third-party monitoring provider
D. Coordinating events with appropriate agencies

Answer: A

NEW QUESTION 921
- (Exam Topic 1)
During an IT risk scenario review session, business executives question why they have been assigned ownership of IT-related risk scenarios. They feel IT risk is technical in nature and therefore should be owned by IT. Which of the following is the BEST way for the risk practitioner to address these concerns?

A. Describe IT risk scenarios in terms of business risk.
B. Recommend the formation of an executive risk council to oversee IT risk.
C. Provide an estimate of IT system downtime if IT risk materializes.
D. Educate business executives on IT risk concepts.

Answer: A

NEW QUESTION 926
- (Exam Topic 1)
Which of the following is MOST important to understand when determining an appropriate risk assessment approach?

A. Complexity of the IT infrastructure
B. Value of information assets
C. Management culture
D. Threats and vulnerabilities

Answer: B

NEW QUESTION 927
- (Exam Topic 1)
Which of the following will BEST quantify the risk associated with malicious users in an organization?

A. Business impact analysis
B. Risk analysis
C. Threat risk assessment
D. Vulnerability assessment

Answer: A

NEW QUESTION 932
- (Exam Topic 1)

After a risk has been identified, who is in the BEST position to select the appropriate risk treatment option?

A. The risk practitioner
B. The business process owner
C. The risk owner
D. The control owner

Answer: C

NEW QUESTION 937
......

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

100% Actual & Verified — Instant Download, Please Click
Order The CRISC Practice Test Here