Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 3)
Which of the following would be a risk practitioner's BEST course of action when a project team has accepted a risk outside the established risk appetite?

A. Reject the risk acceptance and require mitigating controls.
B. Monitor the residual risk level of the accepted risk.
C. Escalate the risk decision to the project sponsor for review.
D. Document the risk decision in the project risk register.

Answer: B

NEW QUESTION 2
- (Exam Topic 3)
Which of the following BEST enables an organization to determine whether external emerging risk factors will impact the organization's risk profile?

A. Control identification and mitigation
B. Adoption of a compliance-based approach
C. Prevention and detection techniques
D. Scenario analysis and stress testing

Answer: D

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

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

Answer: B

NEW QUESTION 4
- (Exam Topic 3)
Which of the following is the MOST important topic to cover in a risk awareness training program for all staff?

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

Answer: C

NEW QUESTION 5
- (Exam Topic 3)
When documenting a risk response, which of the following provides the STRONGEST evidence to support the decision?

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

Answer: C

NEW QUESTION 6
- (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 7
- (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 8
- (Exam Topic 3)
Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

A. A record of incidents is maintained.
B. Forensic investigations are facilitated.
C. Security violations can be identified.
D. Developing threats are detected earlier.

Answer: C

NEW QUESTION 9
- (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 10
- (Exam Topic 3)
Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?

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

Answer: D

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

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

Answer: C

NEW QUESTION 15
- (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 19
- (Exam Topic 3)
Which of the following will BEST help to ensure key risk indicators (KRIs) provide value to risk owners?

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

Answer: B

NEW QUESTION 21
- (Exam Topic 3)
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 25
- (Exam Topic 3)
An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

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

Answer: B

NEW QUESTION 27
- (Exam Topic 3)
Management has required information security awareness training to reduce the risk associated with credential compromise. What is the BEST way to assess the effectiveness of the training?

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

Answer: A

NEW QUESTION 31
- (Exam Topic 3)
The MAIN reason for creating and maintaining a risk register is to:

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

Answer: D

NEW QUESTION 32
- (Exam Topic 3)
During implementation of an intrusion detection system (IDS) to monitor network traffic, a high number of alerts is reported. The risk practitioner should recommend to:

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

Answer: C

NEW QUESTION 33
- (Exam Topic 3)
Which of the following is MOST important to the integrity of a security log?

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

Answer: B

NEW QUESTION 37
- (Exam Topic 3)
An organization moved its payroll system to a Software as a Service (SaaS) application. A new data privacy regulation stipulates that data can only be processed within the country where it is collected. Which of the following should be done FIRST when addressing this situation?

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

Answer: B

NEW QUESTION 38
- (Exam Topic 3)
In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

A. Establishing an intellectual property agreement
B. Evaluating each of the data sources for vulnerabilities
C. Periodically reviewing big data strategies
D. Benchmarking to industry best practice

Answer: B

NEW QUESTION 39
- (Exam Topic 3)
Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

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

Answer: B

NEW QUESTION 41
- (Exam Topic 3)
Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

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

Answer: A

NEW QUESTION 43
- (Exam Topic 3)
An organization planning to transfer and store its customer data with an offshore cloud service provider should be PRIMARILY concerned with:

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

Answer: B

NEW QUESTION 47
- (Exam Topic 3)
Which of the following is the MOST critical element to maximize the potential for a successful security implementation?

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

Answer: C

NEW QUESTION 50
- (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 54
- (Exam Topic 3)
A chief information officer (CIO) has identified risk associated with shadow systems being maintained by business units to address specific functionality gaps in the organization's enterprise resource planning (ERP) system. What is the BEST way to reduce this risk going forward?

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

Answer: B

NEW QUESTION 56
- (Exam Topic 3)
An organization wants to launch a campaign to advertise a new product Using data analytics, the campaign can be targeted to reach potential customers. Which of the following should be of GREATEST concern to the risk practitioner?

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

Answer: D

NEW QUESTION 58
- (Exam Topic 3)
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 61
- (Exam Topic 3)
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 64
- (Exam Topic 3)
Which of the following roles is BEST suited to help a risk practitioner understand the impact of IT-related events on business objectives?

A. IT management
B. Internal audit
C. Process owners
D. Senior management

Answer: C

NEW QUESTION 65
- (Exam Topic 3)
Which of the following is the BEST control to minimize the risk associated with scope creep in software development?

A. An established process for project change management
B. Retention of test data and results for review purposes
C. Business managements review of functional requirements
D. Segregation between development, test, and production

Answer: A

NEW QUESTION 67
- (Exam Topic 3)
An organization has outsourced its billing function to an external service provider. Who should own the risk of customer data leakage caused by the service provider?

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

Answer: D

NEW QUESTION 69
- (Exam Topic 3)
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 74
- (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 78
- (Exam Topic 3)
Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

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

Answer: A

NEW QUESTION 83
- (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 84
- (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 86
- (Exam Topic 3)
Which element of an organization's risk register is MOST important to update following the commissioning of a new financial reporting system?

A. Key risk indicators (KRIs)
B. The owner of the financial reporting process
C. The risk rating of affected financial processes
D. The list of relevant financial controls

Answer: C

NEW QUESTION 88
- (Exam Topic 3)
Which of the following would be a risk practitioner'$ BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

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

Answer: B

NEW QUESTION 93

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

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

Answer: B

NEW QUESTION 96
- (Exam Topic 3)
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 101
- (Exam Topic 3)
Determining if organizational risk is tolerable requires:

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

Answer: D

NEW QUESTION 105
- (Exam Topic 3)
During an acquisition, which of the following would provide the MOST useful input to the parent company's risk practitioner when developing risk scenarios for the post-acquisition phase?

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

Answer: C

NEW QUESTION 106
- (Exam Topic 3)
A bank recently incorporated Blockchain technology with the potential to impact known risk within the organization. Which of the following is the risk practitioner's BEST course of action?

A. Determine whether risk responses are still adequate.
B. Analyze and update control assessments with the new processes.
C. Analyze the risk and update the risk register as needed.
D. Conduct testing of the control that mitigate the existing risk.

Answer: B

NEW QUESTION 107
- (Exam Topic 3)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 108
- (Exam Topic 3)
Which of the following is the MOST important consideration when sharing risk management updates with executive management?

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

Answer: D

NEW QUESTION 109
- (Exam Topic 3)
Which of the following will be the GREATEST concern when assessing the risk profile of an organization?

A. The risk profile was not updated after a recent incident
B. The risk profile was developed without using industry standards.
C. The risk profile was last reviewed two years ago.
D. The risk profile does not contain historical loss data.

Answer: A

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

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

Answer: D

NEW QUESTION 116
- (Exam Topic 3)
When reviewing the business continuity plan (BCP) of an online sales order system, a risk practitioner notices that the recovery time objective (RTO) has a shorter lime than what is defined in the disaster recovery plan (DRP). Which of the following is the BEST way for the risk practitioner to address this concern?

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

Answer: D

NEW QUESTION 117
- (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 120
- (Exam Topic 3)
An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course of action?

A. Report the observation to the chief risk officer (CRO).
B. Validate the adequacy of the implemented risk mitigation measures.
C. Update the risk register with the implemented risk mitigation actions.
D. Revert the implemented mitigation measures until approval is obtained

Answer: B

NEW QUESTION 125
- (Exam Topic 3)
Which of the following is the GREATEST risk associated with the misclassification of data?

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

Answer: A

NEW QUESTION 129
- (Exam Topic 3)
An organization has completed a risk assessment of one of its service providers. Who should be accountable for ensuring that risk responses are implemented?

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

Answer: C

NEW QUESTION 131
- (Exam Topic 3)
Which of the following is the PRIMARY role of a data custodian in the risk management process?

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

Answer: D

NEW QUESTION 134
- (Exam Topic 3)
Which of the following would BEST help an enterprise define and communicate its risk appetite?

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

Answer: C

NEW QUESTION 136
- (Exam Topic 3)
Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

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

Answer: A

NEW QUESTION 138
- (Exam Topic 3)
Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

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

Answer: C

NEW QUESTION 142
- (Exam Topic 3)
The PRIMARY advantage of involving end users in continuity planning is that they:

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

Answer: A

NEW QUESTION 145
- (Exam Topic 3)
Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

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

Answer: A

NEW QUESTION 149
- (Exam Topic 3)
A risk practitioner observed Vial a high number of pokey exceptions were approved by senior management. Which of the following is the risk practitioner's BEST course of action to determine root cause?

A. Review the risk profile

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

Answer: C

NEW QUESTION 150
- (Exam Topic 3)
Which of the following is the MOST common concern associated with outsourcing to a service provider?

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

Answer: C

NEW QUESTION 153
- (Exam Topic 3)
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

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

Answer: D

NEW QUESTION 158
- (Exam Topic 3)
Which of the following is MOST important for an organization to update following a change in legislation requiring notification to individuals impacted by data breaches?

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

Answer: C

NEW QUESTION 160
- (Exam Topic 3)
A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

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

Answer: C

NEW QUESTION 165
- (Exam Topic 3)
The BEST metric to demonstrate that servers are configured securely is the total number of servers:

A. exceeding availability thresholds
B. experiencing hardware failures
C. exceeding current patching standards.
D. meeting the baseline for hardening.

Answer: D

NEW QUESTION 169
- (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 174

- (Exam Topic 3)
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 178
- (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 180
- (Exam Topic 3)
Which of the following controls BEST helps to ensure that transaction data reaches its destination?

A. Securing the network from attacks
B. Providing acknowledgments from receiver to sender
C. Digitally signing individual messages
D. Encrypting data-in-transit

Answer: B

NEW QUESTION 185
- (Exam Topic 3)
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 188
- (Exam Topic 3)
Which of the following methods is an example of risk mitigation?

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

Answer: C

NEW QUESTION 189
- (Exam Topic 3)
Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?

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

Answer: B

NEW QUESTION 191
- (Exam Topic 3)
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 192
- (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 195
- (Exam Topic 3)
Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?

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

Answer: A

NEW QUESTION 199
- (Exam Topic 3)
Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

A. Aligning IT with short-term and long-term goals of the organization
B. Ensuring the IT budget and resources focus on risk management
C. Ensuring senior management's primary focus is on the impact of identified risk
D. Prioritizing internal departments that provide service to customers

Answer: A

NEW QUESTION 202
- (Exam Topic 3)
The BEST way to improve a risk register is to ensure the register:

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

Answer: A

NEW QUESTION 204
- (Exam Topic 3)
An organization is preparing to transfer a large number of customer service representatives to the sales department. Of the following, who is responsible for mitigating the risk associated with residual system access?

A. IT service desk manager
B. Sales manager
C. Customer service manager
D. Access control manager

Answer: D

NEW QUESTION 205
- (Exam Topic 3)
Which of the following should be the MOST important consideration when performing a vendor risk assessment?

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

Answer: B

NEW QUESTION 207
- (Exam Topic 3)
Which of the following should be management's PRIMARY consideration when approving risk response action plans?

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

Answer:

C

NEW QUESTION 208
- (Exam Topic 3)
Which of the following will BEST help to ensure implementation of corrective action plans?

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

Answer: B

NEW QUESTION 212
- (Exam Topic 3)
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

A. Sufficient resources are not assigned to IT development projects.
B. Customer support help desk staff does not have adequate training.
C. Email infrastructure does not have proper rollback plans.
D. The corporate email system does not identify and store phishing emails.

Answer: A

NEW QUESTION 213
- (Exam Topic 3)
Which key performance efficiency IKPI) BEST measures the effectiveness of an organization's disaster recovery program?

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

Answer: D

NEW QUESTION 214
- (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 217
- (Exam Topic 3)
Which of the following will BEST help in communicating strategic risk priorities?

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

Answer: A

NEW QUESTION 219
- (Exam Topic 3)
The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

A. resources to monitor backups
B. restoration monitoring reports
C. backup recovery requests
D. recurring restore failures

Answer: D

NEW QUESTION 220
- (Exam Topic 3)
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 221
- (Exam Topic 3)
Which of the following will be MOST effective in uniquely identifying the originator of electronic transactions?

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

Answer: A

NEW QUESTION 222
- (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 226
- (Exam Topic 3)
Which of the following is MOST important information to review when developing plans for using emerging technologies?

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

Answer: D

NEW QUESTION 231
- (Exam Topic 3)
The MOST important objective of information security controls is to:

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

Answer: C

NEW QUESTION 235
- (Exam Topic 3)
During a risk treatment plan review, a risk practitioner finds the approved risk action plan has not been completed However, there were other risk mitigation actions implemented. Which of the fallowing is the BEST course of action?

A. Review the cost-benefit of mitigating controls
B. Mark the risk status as unresolved within the risk register
C. Verify the sufficiency of mitigating controls with the risk owner
D. Update the risk register with implemented mitigating actions

Answer: A

NEW QUESTION 239
- (Exam Topic 3)
Which of the following should be of GREATEST concern lo a risk practitioner reviewing the implementation of an emerging technology?

A. Lack of alignment to best practices
B. Lack of risk assessment
C. Lack of risk and control procedures
D. Lack of management approval

Answer: B

NEW QUESTION 244
- (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 245
- (Exam Topic 3)
Who should be responsible (of evaluating the residual risk after a compensating control has been

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

Answer: D

NEW QUESTION 250
- (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 251
- (Exam Topic 3)
When evaluating a number of potential controls for treating risk, it is MOST important to consider:

A. risk appetite and control efficiency.
B. inherent risk and control effectiveness.
C. residual risk and cost of control.
D. risk tolerance and control complexity.

Answer: C

NEW QUESTION 253
- (Exam Topic 3)
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

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

Answer: D

NEW QUESTION 258
- (Exam Topic 3)
Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

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

Answer: B

NEW QUESTION 260
- (Exam Topic 3)
Which of the following represents a vulnerability?

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

Answer: C

NEW QUESTION 262

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

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

Answer: D

NEW QUESTION 264
- (Exam Topic 3)
An organization uses a vendor to destroy hard drives. Which of the following would BEST reduce the risk of data leakage?

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

Answer: B

NEW QUESTION 265
- (Exam Topic 3)
Which of the following is MOST important to compare against the corporate risk profile?

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

Answer: D

NEW QUESTION 267
- (Exam Topic 3)
An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

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

Answer: C

NEW QUESTION 268
- (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 269
- (Exam Topic 3)
Which of the following BEST indicates the efficiency of a process for granting access privileges?

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

Answer: C

NEW QUESTION 270
- (Exam Topic 3)
Which of the following statements describes the relationship between key risk indicators (KRIs) and key control indicators (KCIs)?

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

Answer: A

NEW QUESTION 274
- (Exam Topic 3)
To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:

A. require the vendor to sign a nondisclosure agreement
B. clearly define the project scope.
C. perform background checks on the vendor.
D. notify network administrators before testing

Answer: A

NEW QUESTION 277
- (Exam Topic 3)
Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

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

Answer: D

NEW QUESTION 280
- (Exam Topic 3)
Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?

A. Segregation of duties
B. Three lines of defense
C. Compliance review
D. Quality assurance review

Answer: B

NEW QUESTION 281
- (Exam Topic 3)
Which of the following is the BEST way to help ensure risk will be managed properly after a business process has been re-engineered?

A. Reassessing control effectiveness of the process
B. Conducting a post-implementation review to determine lessons learned
C. Reporting key performance indicators (KPIs) for core processes
D. Establishing escalation procedures for anomaly events

Answer: A

NEW QUESTION 283
- (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 287
- (Exam Topic 3)
Which of the following is the GREATEST advantage of implementing a risk management program?

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

Answer: A

NEW QUESTION 288
- (Exam Topic 3)
A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

A. Single sign-on
B. Audit trail review
C. Multi-factor authentication
D. Data encryption at rest

Answer:

B

NEW QUESTION 289
- (Exam Topic 3)
Which of The following is the MOST comprehensive input to the risk assessment process specific to the effects of system downtime?

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

Answer: C

NEW QUESTION 294
- (Exam Topic 3)
The objective of aligning mitigating controls to risk appetite is to ensure that:

A. exposures are reduced to the fullest extent
B. exposures are reduced only for critical business systems
C. insurance costs are minimized
D. the cost of controls does not exceed the expected loss.

Answer: D

NEW QUESTION 297
- (Exam Topic 3)
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 298
- (Exam Topic 3)
Which of the following is the BEST way to assess the effectiveness of an access management process?

A. Comparing the actual process with the documented process
B. Reviewing access logs for user activity
C. Reconciling a list of accounts belonging to terminated employees
D. Reviewing for compliance with acceptable use policy

Answer: B

NEW QUESTION 303
- (Exam Topic 3)
Which of the following is the MOST important reason to link an effective key control indicator (KCI) to relevant key risk indicators (KRIs)?

A. To monitor changes in the risk environment
B. To provide input to management for the adjustment of risk appetite
C. To monitor the accuracy of threshold levels in metrics
D. To obtain business buy-in for investment in risk mitigation measures

Answer: A

NEW QUESTION 304
- (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 306
- (Exam Topic 3)
An organization control environment is MOST effective when:

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

Answer: B

NEW QUESTION 309
- (Exam Topic 3)
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 312
- (Exam Topic 3)
Which of the following provides the MOST useful information to determine risk exposure following control implementations?

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

Answer: C

NEW QUESTION 317
- (Exam Topic 3)
Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

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

Answer: B

NEW QUESTION 321
- (Exam Topic 3)
Which of the following should be the risk practitioner's FIRST course of action when an organization plans to adopt a cloud computing strategy?

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

Answer: B

NEW QUESTION 326
- (Exam Topic 3)
Which of the following should be done FIRST when information is no longer required to support business objectives?

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

Answer: C

NEW QUESTION 328
- (Exam Topic 3)
Which of the following is the MOST important step to ensure regulatory requirements are adequately addressed within an organization?

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

Answer: B

NEW QUESTION 331
- (Exam Topic 3)
Which of the following scenarios represents a threat?

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

D. A virus transmitted on a USB thumb drive

Answer: D

NEW QUESTION 334
- (Exam Topic 3)
When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

A. An analysis of the security logs that illustrate the sequence of events
B. An analysis of the impact of similar attacks in other organizations
C. A business case for implementing stronger logical access controls
D. A justification of corrective action taken

Answer: B

NEW QUESTION 338
- (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 342
- (Exam Topic 3)
A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 343
- (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 345
- (Exam Topic 3)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 346
- (Exam Topic 3)
Before assigning sensitivity levels to information it is MOST important to:

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

Answer: B

NEW QUESTION 350
- (Exam Topic 3)
Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

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

Answer: D

NEW QUESTION 352
- (Exam Topic 3)
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 355
- (Exam Topic 3)
Winch of the following can be concluded by analyzing the latest vulnerability report for the it infrastructure?

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

Answer: C

NEW QUESTION 360
- (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 363
- (Exam Topic 3)
Which of the following is the STRONGEST indication an organization has ethics management issues?

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

Answer: A

NEW QUESTION 365
- (Exam Topic 3)
An IT department originally planned to outsource the hosting of its data center at an overseas location to reduce operational expenses. After a risk assessment, the department has decided to keep the data center in-house. How should the risk treatment response be reflected in the risk register?

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

Answer: A

NEW QUESTION 370
- (Exam Topic 3)
Which of the following is the BEST method of creating risk awareness in an organization?

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

Answer: B

NEW QUESTION 375

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

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

Answer: C

NEW QUESTION 378
- (Exam Topic 3)
An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

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

Answer: B

NEW QUESTION 379
- (Exam Topic 3)
Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

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

Answer: B

NEW QUESTION 384
- (Exam Topic 3)
A service provider is managing a client's servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider's MOST appropriate action would be to:

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

Answer: D

NEW QUESTION 388
- (Exam Topic 3)
Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

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

Answer: C

NEW QUESTION 389
- (Exam Topic 3)
An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate tins risk?

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

Answer: C

NEW QUESTION 392
- (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 397
- (Exam Topic 2)
Which of the following is the PRIMARY role of the board of directors in corporate risk governance?

A. Approving operational strategies and objectives
B. Monitoring the results of actions taken to mitigate risk
C. Ensuring the effectiveness of the risk management program
D. Ensuring risk scenarios are identified and recorded in the risk register

Answer: C

NEW QUESTION 402
- (Exam Topic 2)
An organization's internal audit department is considering the implementation of robotics process automation (RPA) to automate certain continuous auditing tasks. Who would own the risk associated with ineffective design of the software bots?

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

Answer: C

NEW QUESTION 403
- (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 407
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is
aligned to business requirements?

A. Total cost to support the policy
B. Number of exceptions to the policy
C. Total cost of policy breaches
D. Number of inquiries regarding the policy

Answer: C

NEW QUESTION 410
- (Exam Topic 2)
A recent internal risk review reveals the majority of core IT application recovery time objectives (RTOs) have exceeded the maximum time defined by the business application owners. Which of the following is MOST likely to change as a result?

A. Risk forecasting
B. Risk tolerance
C. Risk likelihood
D. Risk appetite

Answer: B

NEW QUESTION 414
- (Exam Topic 2)
Which of the following is MOST influential when management makes risk response decisions?

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

Answer: A

NEW QUESTION 419
- (Exam Topic 2)
The MAIN purpose of a risk register is to:

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

Answer: C

NEW QUESTION 420
- (Exam Topic 2)
Which of the following is performed after a risk assessment is completed?

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

Answer: C

NEW QUESTION 421
- (Exam Topic 2)
The MOST important reason to aggregate results from multiple risk assessments on interdependent information systems is to:

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

Answer: A

NEW QUESTION 424
- (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 426
- (Exam Topic 2)
Which of the following criteria is MOST important when developing a response to an attack that would compromise data?

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

Answer: D

NEW QUESTION 431
- (Exam Topic 2)
Which of the following would present the GREATEST challenge when assigning accountability for control ownership?

A. Weak governance structures
B. Senior management scrutiny
C. Complex regulatory environment
D. Unclear reporting relationships

Answer: D

NEW QUESTION 434
- (Exam Topic 2)
Which of the following is MOST important when developing risk scenarios?

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

Answer: C

NEW QUESTION 435
- (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 437
- (Exam Topic 2)
Which of the following would qualify as a key performance indicator (KPI)?

A. Aggregate risk of the organization
B. Number of identified system vulnerabilities
C. Number of exception requests processed in the past 90 days
D. Number of attacks against the organization's website

Answer: B

NEW QUESTION 438
- (Exam Topic 2)
Which of the following activities is PRIMARILY the responsibility of senior management?

A. Bottom-up identification of emerging risks
B. Categorization of risk scenarios against a standard taxonomy
C. Prioritization of risk scenarios based on severity
D. Review of external loss data

Answer: C

NEW QUESTION 442
- (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 447
- (Exam Topic 2)
A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?

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

Answer: D

NEW QUESTION 449
- (Exam Topic 2)
The PRIMARY benefit of classifying information assets is that it helps to:

A. communicate risk to senior management
B. assign risk ownership
C. facilitate internal audit
D. determine the appropriate level of control

Answer: D

NEW QUESTION 450
- (Exam Topic 2)
A department has been granted an exception to bypass the existing approval process for purchase orders. The risk practitioner should verify the exception has been approved by which of the following?

A. Internal audit
B. Control owner
C. Senior management
D. Risk manager

Answer: B

NEW QUESTION 452
- (Exam Topic 2)

Which of the following would provide the MOST comprehensive information for updating an organization's risk register?

A. Results of the latest risk assessment
B. Results of a risk forecasting analysis
C. A review of compliance regulations
D. Findings of the most recent audit

Answer: A

NEW QUESTION 454
- (Exam Topic 2)
Which of the following would BEST help secure online financial transactions from improper users?

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

Answer: D

NEW QUESTION 459
- (Exam Topic 2)
After identifying new risk events during a project, the project manager s NEXT step should be to:

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

Answer: B

NEW QUESTION 460
- (Exam Topic 2)
Which of the following should be considered FIRST when assessing risk associated with the adoption of emerging technologies?

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

Answer: A

NEW QUESTION 462
- (Exam Topic 2)
An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

A. Review the risk identification process.
B. Inform the risk scenario owners.
C. Create a risk awareness communication plan.
D. Update the risk register.

Answer: A

NEW QUESTION 464
- (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 466
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to consider when evaluating plans for changes to IT services?

A. Change testing schedule
B. Impact assessment of the change
C. Change communication plan
D. User acceptance testing (UAT)

Answer: B

NEW QUESTION 468

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

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

Answer: D

NEW QUESTION 472
- (Exam Topic 2)
Which of the following is the MOST effective way to integrate business risk management with IT operations?

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

Answer: D

NEW QUESTION 474
- (Exam Topic 2)
Prior to selecting key performance indicators (KPIs), itis MOST important to ensure:

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

Answer: C

NEW QUESTION 479
- (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 484
- (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 486
- (Exam Topic 2)
What should a risk practitioner do FIRST upon learning a risk treatment owner has implemented a different control than what was specified in the IT risk action plan?

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

Answer: C

NEW QUESTION 488
- (Exam Topic 2)
Which of the following is the GREATEST concern associated with business end users developing their own applications on end user spreadsheets and database programs?

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

Answer: C

NEW QUESTION 491
- (Exam Topic 2)
Which of the following is MOST important for a risk practitioner to update when a software upgrade renders an existing key control ineffective?

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

Answer: C

NEW QUESTION 492
- (Exam Topic 2)
Which of the following is MOST helpful to management when determining the resources needed to mitigate a risk?

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

Answer: C

NEW QUESTION 494
- (Exam Topic 2)
A bank is experiencing an increasing incidence of customer identity theft. Which of the following is the BEST way to mitigate this risk?

A. Implement monitoring techniques.
B. Implement layered security.
C. Outsource to a local processor.
D. Conduct an awareness campaign.

Answer: B

NEW QUESTION 497
- (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 499
- (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 501
- (Exam Topic 2)
Which of the following is the PRIMARY objective for automating controls?

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

Answer: A

NEW QUESTION 503
- (Exam Topic 2)
Which of the following will BEST help to ensure that information system controls are effective?

A. Responding promptly to control exceptions

B. Implementing compensating controls
C. Testing controls periodically
D. Automating manual controls

Answer: C

NEW QUESTION 504
- (Exam Topic 2)
The PRIMARY reason for establishing various Threshold levels for a set of key risk indicators (KRIs) is to:

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

Answer: B

NEW QUESTION 505
- (Exam Topic 2)
A control owner identifies that the organization's shared drive contains personally identifiable information (PII) that can be accessed by all personnel. Which of the following is the MOST effective risk response?

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

Answer: A

NEW QUESTION 508
- (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 510
- (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 514
- (Exam Topic 2)
Which of the following will BEST support management repotting on risk?

A. Risk policy requirements
B. A risk register
C. Control self-assessment
D. Key performance Indicators

Answer: B

NEW QUESTION 517
- (Exam Topic 2)
The effectiveness of a control has decreased. What is the MOST likely effect on the associated risk?

A. The risk impact changes.
B. The risk classification changes.
C. The inherent risk changes.
D. The residual risk changes.

Answer: D

NEW QUESTION 519
- (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 521
- (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 526
- (Exam Topic 2)
Which of the following is the BEST way to support communication of emerging risk?

A. Update residual risk levels to reflect the expected risk impact.
B. Adjust inherent risk levels upward.
C. Include it on the next enterprise risk committee agenda.
D. Include it in the risk register for ongoing monitoring.

Answer: D

NEW QUESTION 527
- (Exam Topic 2)
Which of the following is MOST commonly compared against the risk appetite?

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

Answer: D

NEW QUESTION 530
- (Exam Topic 2)
Which of the following is the MOST important input when developing risk scenarios?

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

Answer: B

NEW QUESTION 532
- (Exam Topic 2)
A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (PII). Which of the following will MOST likely outcome for an organization affected by the new law?

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

Answer: B

NEW QUESTION 536
- (Exam Topic 2)
An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

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

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

Answer: A

NEW QUESTION 540
- (Exam Topic 2)
A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?

A. Reviewing access control lists
B. Authorizing user access requests
C. Performing user access recertification
D. Terminating inactive user access

Answer: B

NEW QUESTION 543
- (Exam Topic 2)
Which of these documents is MOST important to request from a cloud service provider during a vendor risk assessment?

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

Answer: B

NEW QUESTION 545
- (Exam Topic 2)
An organization has just implemented changes to close an identified vulnerability that impacted a critical business process. What should be the NEXT course of action?

A. Redesign the heat map.
B. Review the risk tolerance.
C. Perform a business impact analysis (BIA)
D. Update the risk register.

Answer: D

NEW QUESTION 547
- (Exam Topic 2)
Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?

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

Answer: A

NEW QUESTION 552
- (Exam Topic 2)
An organization is measuring the effectiveness of its change management program to reduce the number of unplanned production changes. Which of the following would be the BEST metric to determine if the program is performing as expected?

A. Decrease in the time to move changes to production
B. Ratio of emergency fixes to total changes
C. Ratio of system changes to total changes
D. Decrease in number of changes without a fallback plan

Answer: B

NEW QUESTION 555
- (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 556
- (Exam Topic 2)
Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?

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

Answer: D

NEW QUESTION 559
- (Exam Topic 2)
Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?

A. The KRIs' source data lacks integrity.
B. The KRIs are not automated.
C. The KRIs are not quantitative.
D. The KRIs do not allow for trend analysis.

Answer: A

NEW QUESTION 561
- (Exam Topic 2)
When assessing the maturity level of an organization's risk management framework, which of the following deficiencies should be of GREATEST concern to a risk practitioner?

A. Unclear organizational risk appetite
B. Lack of senior management participation
C. Use of highly customized control frameworks
D. Reliance on qualitative analysis methods

Answer: C

NEW QUESTION 565
- (Exam Topic 2)
Which of the following will provide the BEST measure of compliance with IT policies?

A. Evaluate past policy review reports.
B. Conduct regular independent reviews.
C. Perform penetration testing.
D. Test staff on their compliance responsibilities.

Answer: C

NEW QUESTION 570
- (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 571
- (Exam Topic 2)
Which of the following MUST be assessed before considering risk treatment options for a scenario with significant impact?

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

Answer: D

NEW QUESTION 576
- (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 578
- (Exam Topic 2)
Who is PRIMARILY accountable for risk treatment decisions?

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

Answer: A

NEW QUESTION 581
- (Exam Topic 2)
Which of the following is the GREATEST concern when using a generic set of IT risk scenarios for risk analysis?

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

Answer: B

NEW QUESTION 583
- (Exam Topic 2)
An organization striving to be on the leading edge in regard to risk monitoring would MOST likely implement:

A. procedures to monitor the operation of controls.
B. a tool for monitoring critical activities and controls.
C. real-time monitoring of risk events and control exceptions.
D. monitoring activities for all critical assets.
E. Perform a controls assessment.

Answer: C

NEW QUESTION 586
- (Exam Topic 2)
An organization plans to migrate sensitive information to a public cloud infrastructure. Which of the following is the GREATEST security risk in this scenario?

A. Data may be commingled with other tenants' data.
B. System downtime does not meet the organization's thresholds.
C. The infrastructure will be managed by the public cloud administrator.
D. The cloud provider is not independently certified.

Answer: A

NEW QUESTION 588
- (Exam Topic 2)
What is the GREATEST concern with maintaining decentralized risk registers instead of a consolidated risk register?

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

Answer: C

NEW QUESTION 589
- (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 592
- (Exam Topic 2)
Which of the following is the GREATEST risk associated with the transition of a sensitive data backup solution from on-premise to a cloud service provider?

A. More complex test restores
B. Inadequate service level agreement (SLA) with the provider

C. More complex incident response procedures
D. Inadequate data encryption

Answer: D

NEW QUESTION 595
- (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 600
- (Exam Topic 2)
Which of the following can be interpreted from a single data point on a risk heat map?

A. Risk tolerance
B. Risk magnitude
C. Risk response
D. Risk appetite

Answer: B

NEW QUESTION 605
- (Exam Topic 2)
Which of the following is the MOST important reason to create risk scenarios?

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

Answer: A

NEW QUESTION 608
- (Exam Topic 2)
Read" rights to application files in a controlled server environment should be approved by the:

A. business process owner.
B. database administrator.
C. chief information officer.
D. systems administrator.

Answer: A

NEW QUESTION 610
- (Exam Topic 2)
The GREATEST concern when maintaining a risk register is that:

A. impacts are recorded in qualitative terms.
B. executive management does not perform periodic reviews.
C. IT risk is not linked with IT assets.
D. significant changes in risk factors are excluded.

Answer: D

NEW QUESTION 613
- (Exam Topic 2)
Which of the following BEST facilitates the development of effective IT risk scenarios?

A. Utilization of a cross-functional team
B. Participation by IT subject matter experts
C. Integration of contingency planning
D. Validation by senior management

Answer: A

NEW QUESTION 618
- (Exam Topic 2)
Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

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

Answer: B

NEW QUESTION 619
- (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 623
- (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 626
- (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 627
- (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 631
- (Exam Topic 2)
When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:

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

Answer: B

NEW QUESTION 633
- (Exam Topic 2)
When prioritizing risk response, management should FIRST:

A. evaluate the organization s ability and expertise to implement the solution.
B. evaluate the risk response of similar organizations.
C. address high risk factors that have efficient and effective solutions.
D. determine which risk factors have high remediation costs

Answer: C

NEW QUESTION 634
- (Exam Topic 2)

An organization has decided to outsource a web application, and customer data will be stored in the vendor's public cloud. To protect customer data, it is MOST important to ensure which of the following?

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

Answer: D

NEW QUESTION 637
- (Exam Topic 2)
Which of the following is the BEST indication that an organization's risk management program has not reached the desired maturity level?

A. Significant increases in risk mitigation budgets
B. Large fluctuations in risk ratings between assessments
C. A steady increase in the time to recover from incidents
D. A large number of control exceptions

Answer: B

NEW QUESTION 641
- (Exam Topic 2)
A control owner has completed a year-long project To strengthen existing controls. It is MOST important for the risk practitioner to:

A. update the risk register to reflect the correct level of residual risk.
B. ensure risk monitoring for the project is initiated.
C. conduct and document a business impact analysis (BIA).
D. verify cost-benefit of the new controls being implemented.

Answer: A

NEW QUESTION 646
- (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 648
- (Exam Topic 2)
Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?

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

Answer: A

NEW QUESTION 649
- (Exam Topic 2)
Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?

A. Establishing a risk management committee
B. Updating the organization's risk register to reflect the new threat
C. Communicating the results of the threat impact analysis
D. Establishing metrics to assess the effectiveness of the responses

Answer: C

NEW QUESTION 652
- (Exam Topic 2)
What can be determined from the risk scenario chart?

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

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

Answer: A

NEW QUESTION 655
- (Exam Topic 2)
Which of the following is the GREATEST risk associated with the use of data analytics?

A. Distributed data sources
B. Manual data extraction
C. Incorrect data selection
D. Excessive data volume

Answer: C

NEW QUESTION 656
- (Exam Topic 1)
A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:

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

Answer: D

NEW QUESTION 659
- (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 660
- (Exam Topic 3)
Which of the following is the GREATEST benefit for an organization with a strong risk awareness culture?

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

Answer: D

NEW QUESTION 663
- (Exam Topic 3)
An organization outsources the processing of us payroll data A risk practitioner identifies a control weakness at the third party trial exposes the payroll data. Who should own this risk?

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

Answer: B

NEW QUESTION 667
- (Exam Topic 3)
An organization has been notified that a disgruntled, terminated IT administrator has tried to break into the corporate network. Which of the following discoveries should be of GREATEST concern to the organization?

A. Authentication logs have been disabled.
B. An external vulnerability scan has been detected.
C. A brute force attack has been detected.
D. An increase in support requests has been observed.

Answer: A

NEW QUESTION 668

- (Exam Topic 3)
Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

A. Implement segregation of duties.
B. Enforce an internal data access policy.
C. Enforce the use of digital signatures.
D. Apply single sign-on for access control.

Answer: B

NEW QUESTION 672
- (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 673
- (Exam Topic 3)
The MOST important reason for implementing change control procedures is to ensure:

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

Answer: A

NEW QUESTION 674
- (Exam Topic 3)
Which of the following is MOST important to include in a risk assessment of an emerging technology?

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

Answer: D

NEW QUESTION 675
- (Exam Topic 3)
Which of the following poses the GREATEST risk to an organization's operations during a major it transformation?

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

Answer: D

NEW QUESTION 676
- (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 679
- (Exam Topic 3)
Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

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

Answer: B

NEW QUESTION 680
- (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 684
- (Exam Topic 3)
Which of the following criteria associated with key risk indicators (KRIs) BEST enables effective risk monitoring?

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

Answer: C

NEW QUESTION 688
- (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 689
- (Exam Topic 3)
A risk practitioner has just learned about new malware that has severely impacted industry peers worldwide data loss?

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

Answer: B

NEW QUESTION 694
- (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 695
- (Exam Topic 3)
A company has recently acquired a customer relationship management (CRM) application from a certified software vendor. Which of the following will BE ST help
lo prevent technical vulnerabilities from being exploded?

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

Answer: D

NEW QUESTION 698
- (Exam Topic 3)
Which of the following will BEST help to ensure the continued effectiveness of the IT risk management function within an organization experiencing high employee
turnover?

A. Well documented policies and procedures
B. Risk and issue tracking
C. An IT strategy committee
D. Change and release management

Answer: B

NEW QUESTION 701
- (Exam Topic 3)
A risk practitioner has collaborated with subject matter experts from the IT department to develop a large list of potential key risk indicators (KRIs) for all IT operations within the organization Of the following, who should review the completed list and select the appropriate KRIs for implementation?

A. IT security managers
B. IT control owners
C. IT auditors
D. IT risk owners

Answer: D

NEW QUESTION 706
- (Exam Topic 3)
Which of the following data would be used when performing a business impact analysis (BIA)?

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

Answer: D

NEW QUESTION 710
- (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 712
- (Exam Topic 3)
Which of the following is MOST important to the successful development of IT risk scenarios?

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

Answer: C

NEW QUESTION 714
- (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 717
- (Exam Topic 3)
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 721
- (Exam Topic 3)
The MAIN purpose of reviewing a control after implementation is to validate that the control:

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

Answer: A

NEW QUESTION 725
- (Exam Topic 3)
When is the BEST to identify risk associated with major project to determine a mitigation plan?

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

Answer: D

NEW QUESTION 729
- (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 734
- (Exam Topic 3)
The risk associated with an asset after controls are applied can be expressed as:

A. a function of the cost and effectiveness of controls.
B. the likelihood of a given threat.
C. a function of the likelihood and impact.
D. the magnitude of an impact.

Answer: C

NEW QUESTION 737
- (Exam Topic 3)
When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

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

Answer: D

NEW QUESTION 741
- (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 742
- (Exam Topic 3)
Prudent business practice requires that risk appetite not exceed:

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

Answer: C

NEW QUESTION 745

- (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 746
- (Exam Topic 3)
A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

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

Answer: A

NEW QUESTION 751
- (Exam Topic 3)
Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

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

Answer: C

NEW QUESTION 753
- (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 758
- (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 763
- (Exam Topic 3)
In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

A. two-factor authentication.
B. continuous data backup controls.
C. encryption for data at rest.
D. encryption for data in motion.

Answer: B

NEW QUESTION 766
- (Exam Topic 2)
Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?

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

Answer: A

NEW QUESTION 768
- (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 771
- (Exam Topic 2)
Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

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

Answer: D

NEW QUESTION 775
- (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 776
- (Exam Topic 2)
During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?

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

Answer: A

NEW QUESTION 781
- (Exam Topic 2)
Which of the following is MOST important to review when determining whether a potential IT service provider's control environment is effective?

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

Answer: A

NEW QUESTION 783
- (Exam Topic 2)
Which of the following should be a risk practitioner's MOST important consideration when developing IT risk scenarios?

A. The impact of controls on the efficiency of the business in delivering services
B. Linkage of identified risk scenarios with enterprise risk management
C. Potential threats and vulnerabilities that may have an impact on the business
D. Results of network vulnerability scanning and penetration testing

Answer: C

NEW QUESTION 784
- (Exam Topic 2)
Which of the following is a KEY outcome of risk ownership?

A. Risk responsibilities are addressed.
B. Risk-related information is communicated.
C. Risk-oriented tasks are defined.
D. Business process risk is analyzed.

Answer: A

NEW QUESTION 788
- (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: B

NEW QUESTION 793
- (Exam Topic 2)
A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

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

Answer: A

NEW QUESTION 795
- (Exam Topic 2)
An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?

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

Answer: A

NEW QUESTION 798
- (Exam Topic 2)
Which of the following is MOST likely to be impacted as a result of a new policy which allows staff members to remotely connect to the organization's IT systems via personal or public computers?

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

Answer: B

NEW QUESTION 799
- (Exam Topic 2)
Which of the following is the FIRST step when developing a business case to drive the adoption of a risk remediation project by senior management?

A. Calculating the cost
B. Analyzing cost-effectiveness
C. Determining the stakeholders
D. Identifying the objectives

Answer: A

NEW QUESTION 803
- (Exam Topic 2)
An organization has implemented a system capable of comprehensive employee monitoring. Which of the following should direct how the system is used?

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

Answer: D

NEW QUESTION 805
- (Exam Topic 2)
When reviewing a risk response strategy, senior management's PRIMARY focus should be placed on the:

A. cost-benefit analysis.
B. investment portfolio.
C. key performance indicators (KPIs).
D. alignment with risk appetite.

Answer: D

NEW QUESTION 809
- (Exam Topic 2)
An organization is considering adopting artificial intelligence (AI). Which of the following is the risk practitioner's MOST important course of action?

A. Develop key risk indicators (KRIs).
B. Ensure sufficient pre-implementation testing.
C. Identify applicable risk scenarios.
D. Identify the organization's critical data.

Answer: C

NEW QUESTION 812
- (Exam Topic 2)
A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration when establishing a contingency plan and an alternate processing site?

A. The alternative site is a hot site with equipment ready to resume processing immediately.
B. The contingency plan provides for backup media to be taken to the alternative site.
C. The contingency plan for high priority applications does not involve a shared cold site.
D. The alternative site does not reside on the same fault to matter how the distance apart.

Answer: B

NEW QUESTION 814
- (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 818
- (Exam Topic 2)
Which of the following BEST promotes commitment to controls?

A. Assigning control ownership
B. Assigning appropriate resources
C. Assigning a quality control review
D. Performing regular independent control reviews

Answer: A

NEW QUESTION 819
- (Exam Topic 2)
Which of the following would be the GREATEST concern related to data privacy when implementing an Internet of Things (IoT) solution that collects personally identifiable information (PII)?

A. A privacy impact assessment has not been completed.
B. Data encryption methods apply to a subset of PII obtained.
C. The data privacy officer was not consulted.
D. Insufficient access controls are used on the IoT devices.

Answer: A

NEW QUESTION 824
- (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 825

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

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

Answer: A

NEW QUESTION 830
- (Exam Topic 2)
Which of the following observations would be GREATEST concern to a risk practitioner reviewing the implementation status of management action plans?

A. Management has not determined a final implementation date.
B. Management has not completed an early mitigation milestone.
C. Management has not secured resources for mitigation activities.
D. Management has not begun the implementation.

Answer: C

NEW QUESTION 833
- (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 834
- (Exam Topic 2)
Quantifying the value of a single asset helps the organization to understand the:

A. overall effectiveness of risk management
B. consequences of risk materializing
C. necessity of developing a risk strategy,
D. organization s risk threshold.

Answer: B

NEW QUESTION 835
- (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 838
- (Exam Topic 2)
Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?

A. Self-assessments by process owners
B. Mitigation plan progress reports
C. Risk owner attestation
D. Change in the level of residual risk

Answer: D

NEW QUESTION 839
- (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 843
- (Exam Topic 2)
A large organization is replacing its enterprise resource planning (ERP) system and has decided not to deploy the payroll module of the new system. Instead, the current payroll system will continue to be
used. Of the following, who should own the risk if the ERP and payroll system fail to operate as expected?

A. The business owner
B. The ERP administrator
C. The project steering committee
D. The IT project manager

Answer: A

NEW QUESTION 844
- (Exam Topic 1)
Which of the following risk register updates is MOST important for senior management to review?

A. Extending the date of a future action plan by two months
B. Retiring a risk scenario no longer used
C. Avoiding a risk that was previously accepted
D. Changing a risk owner

Answer: A

NEW QUESTION 847
- (Exam Topic 1)
A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application. Who should have the authority to accept the associated risk?

A. Business continuity director
B. Disaster recovery manager
C. Business application owner
D. Data center manager

Answer: C

NEW QUESTION 851
- (Exam Topic 1)
Which of the following would be a risk practitioners BEST recommendation for preventing cyber intrusion?

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

Answer: D

NEW QUESTION 855
......

Relate Links

100% Pass Your CRISC Exam with Exambible Prep Materials

https://www.exambible.com/CRISC-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/