Exam Questions CRISC

Certified in Risk and Information Systems Control

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

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

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

Answer: C

NEW QUESTION 2
- (Exam Topic 4)
When classifying and prioritizing risk responses, the areas to address FIRST are those with:

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

Answer: C

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

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

Answer: B

NEW QUESTION 4
- (Exam Topic 4)
A highly regulated enterprise is developing a new risk management plan to specifically address legal and regulatory risk scenarios What should be done FIRST by IT governance to support this effort?

A. Request a regulatory risk reporting methodology
B. Require critical success factors (CSFs) for IT risks.
C. Establish IT-specific compliance objectives
D. Communicate IT key risk indicators (KRIs) and triggers

Answer: A

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

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

Answer: B

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

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

Answer: C

NEW QUESTION 7
- (Exam Topic 4)
Which of the following key performance indicators (KPis) would BEST measure me risk of a service outage when using a Software as a Service (SaaS) vendors

A. Frequency of business continuity plan (BCP) lasting
B. Frequency and number of new software releases

C. Frequency and duration of unplanned downtime
D. Number of IT support staff available after business hours

Answer: C

NEW QUESTION 8
- (Exam Topic 4)
Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

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

Answer: A

NEW QUESTION 9
- (Exam Topic 4)
An organization is considering outsourcing user administration controls tor a critical system. The potential vendor has offered to perform quarterly sett-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to me risk practitioner?

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

Answer: D

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

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

Answer: B

NEW QUESTION 10
- (Exam Topic 4)
Which component of a software inventory BEST enables the identification and mitigation of known vulnerabilities?

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

Answer: A

NEW QUESTION 14
- (Exam Topic 4)
Which of the following is PRIMARILY a risk management responsibly of the first line of defense?

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

Answer: C

NEW QUESTION 17
- (Exam Topic 4)
Which of the following would provide the BEST evidence of an effective internal control environment/?

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

Answer: D

NEW QUESTION 19
- (Exam Topic 4)

Which of the following is the PRIMARY reason for a risk practitioner to review an organization's IT asset inventory?

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

Answer: C

NEW QUESTION 20
- (Exam Topic 4)
Which of the following practices would be MOST effective in protecting personality identifiable information
(Ptl) from unauthorized access m a cloud environment?

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

Answer: B

NEW QUESTION 21
- (Exam Topic 4)
An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis Which of the following is the MOST important control to ensure the privacy of customer information?

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

Answer: C

NEW QUESTION 26
- (Exam Topic 4)
What is senior management's role in the RACI model when tasked with reviewing monthly status reports provided by risk owners?

A. Accountable
B. Informed
C. Responsible
D. Consulted

Answer: B

NEW QUESTION 30
- (Exam Topic 4)
Which of the following is the MOST effective way to help ensure accountability for managing risk?

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

Answer: A

NEW QUESTION 32
- (Exam Topic 4)
Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

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

Answer: A

NEW QUESTION 34
- (Exam Topic 4)
A multinational organization is considering implementing standard background checks to' all new employees A KEY concern regarding this approach

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

Answer: C

NEW QUESTION 35
- (Exam Topic 3)
The PRIMARY reason for prioritizing risk scenarios is to:

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

Answer: D

NEW QUESTION 36
- (Exam Topic 4)
Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?

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

Answer: A

NEW QUESTION 39
- (Exam Topic 4)
Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?

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

Answer: D

NEW QUESTION 44
- (Exam Topic 4)
A penetration test reveals several vulnerabilities in a web-facing application. Which of the following should be the FIRST step in selecting a risk response?

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

Answer: C

NEW QUESTION 47
- (Exam Topic 3)
Which of the following provides the BEST evidence that a selected risk treatment plan is effective?

A. Identifying key risk indicators (KRIs)
B. Evaluating the return on investment (ROI)
C. Evaluating the residual risk level
D. Performing a cost-benefit analysis

Answer: D

NEW QUESTION 50
- (Exam Topic 3)
Which of the following is the BEST way to determine the potential organizational impact of emerging privacy regulations?

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

Answer: D

NEW QUESTION 54
- (Exam Topic 3)
Which of the following is MOST useful when communicating risk to management?

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

Answer: C

NEW QUESTION 59
- (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 61
- (Exam Topic 3)
Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?

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

Answer: D

NEW QUESTION 65
- (Exam Topic 3)
Which of the following is MOST helpful in preventing risk events from materializing?

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

Answer: A

NEW QUESTION 68
- (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 73
- (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 75
- (Exam Topic 3)
Which of the following should be considered when selecting a risk response?

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

Answer: B

NEW QUESTION 79
- (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 84
- (Exam Topic 3)
The PRIMARY purpose of using a framework for risk analysis is to:

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

Answer: B

NEW QUESTION 88
- (Exam Topic 3)
When developing a new risk register, a risk practitioner should focus on which of the following risk management activities?

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

Answer: C

NEW QUESTION 93
- (Exam Topic 3)
Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?

A. Evaluating the impact to control objectives
B. Conducting a root cause analysis
C. Validating the adequacy of current processes
D. Reconfiguring the IT infrastructure

Answer: B

NEW QUESTION 95
- (Exam Topic 3)
Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

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

Answer: D

NEW QUESTION 100
- (Exam Topic 3)
Which of the following is the MOST important responsibility of a risk owner?

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

Answer: C

NEW QUESTION 102
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?

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

Answer: D

NEW QUESTION 107
- (Exam Topic 3)
Which of the following is the MOST appropriate action when a tolerance threshold is exceeded?

A. Communicate potential impact to decision makers.
B. Research the root cause of similar incidents.

C. Verify the response plan is adequate.
D. Increase human resources to respond in the interim.

Answer: A

NEW QUESTION 109
- (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 112
- (Exam Topic 3)
Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

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

Answer: C

NEW QUESTION 113
- (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 115
- (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 119
- (Exam Topic 3)
When of the following provides the MOST tenable evidence that a business process control is effective?

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

Answer: C

NEW QUESTION 121
- (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 125
- (Exam Topic 3)

Which of the following should be determined FIRST when a new security vulnerability is made public?

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

Answer: A

NEW QUESTION 129
- (Exam Topic 3)
While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

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

Answer: B

NEW QUESTION 131
- (Exam Topic 3)
When of the following is the MOST significant exposure when an application uses individual user accounts to access the underlying database?

A. Users may share accounts with business system analyst
B. Application may not capture a complete audit trail.
C. Users may be able to circumvent application controls.
D. Multiple connects to the database are used and slow the process

Answer: C

NEW QUESTION 134
- (Exam Topic 3)
An organization discovers significant vulnerabilities in a recently purchased commercial off-the-shelf software product which will not be corrected until the next release. Which of the following is the risk manager's BEST course of action?

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

Answer: C

NEW QUESTION 138
- (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 143
- (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 146
- (Exam Topic 3)
Which of the following should be included in a risk scenario to be used for risk analysis?

A. Risk appetite
B. Threat type
C. Risk tolerance
D. Residual risk

Answer: B

NEW QUESTION 150
- (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 154
- (Exam Topic 3)
Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information lo a supplier?

A. Encrypt the data while in transit lo the supplier
B. Contractually obligate the supplier to follow privacy laws.
C. Require independent audits of the supplier's control environment
D. Utilize blockchain during the data transfer

Answer: B

NEW QUESTION 156
- (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 157
- (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 160
- (Exam Topic 3)
Which of the following will BEST support management reporting on risk?

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

Answer: C

NEW QUESTION 161
- (Exam Topic 3)
Reviewing historical risk events is MOST useful for which of the following processes within the risk management life cycle?

A. Risk monitoring
B. Risk mitigation
C. Risk aggregation
D. Risk assessment

Answer: D

NEW QUESTION 166
- (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 170
- (Exam Topic 3)
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

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

Answer: C

NEW QUESTION 175
- (Exam Topic 3)
While reviewing the risk register, a risk practitioner notices that different business units have significant variances in inherent risk for the same risk scenario. Which of the following is the BEST course of action?

A. Update the risk register with the average of residual risk for both business units.
B. Review the assumptions of both risk scenarios to determine whether the variance is reasonable.
C. Update the risk register to ensure both risk scenarios have the highest residual risk.
D. Request that both business units conduct another review of the risk.

Answer: B

NEW QUESTION 177
- (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 182
- (Exam Topic 3)
Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?

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

Answer: C

NEW QUESTION 187
- (Exam Topic 3)
Which of the following is the BEST reason to use qualitative measures to express residual risk levels related to emerging threats?

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

Answer: C

NEW QUESTION 190
- (Exam Topic 3)
An organization is conducting a review of emerging risk. Which of the following is the BEST input for this exercise?

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

Answer: B

NEW QUESTION 194
- (Exam Topic 3)
Which of the following would be MOST helpful to a risk practitioner when ensuring that mitigated risk remains within acceptable limits?

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

D. Implementing a process for ongoing monitoring of control effectiveness

Answer: D

NEW QUESTION 196
- (Exam Topic 3)
Which of the following practices MOST effectively safeguards the processing of personal data?

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

Answer: B

NEW QUESTION 197
- (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 198
- (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 203
- (Exam Topic 3)
A business unit is implementing a data analytics platform to enhance its customer relationship management (CRM) system primarily to process data that has been provided by its customers. Which of the following presents the GREATEST risk to the organization's reputation?

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

Answer: B

NEW QUESTION 208
- (Exam Topic 3)
Which of the following is the MOST important consideration for protecting data assets m a Business application system?

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

Answer: A

NEW QUESTION 213
- (Exam Topic 3)
Legal and regulatory risk associated with business conducted over the Internet is driven by:

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

Answer: C

NEW QUESTION 217
- (Exam Topic 3)
An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?

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

Answer: B

NEW QUESTION 219
- (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 224
- (Exam Topic 3)
To reduce costs, an organization is combining the second and third tines of defense in a new department that reports to a recently appointed C-level executive. Which of the following is the GREATEST concern with this situation?

A. The risk governance approach of the second and third lines of defense may differ.
B. The independence of the internal third line of defense may be compromised.
C. Cost reductions may negatively impact the productivity of other departments.
D. The new structure is not aligned to the organization's internal control framework.

Answer: B

NEW QUESTION 228
- (Exam Topic 3)
Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

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

Answer: D

NEW QUESTION 232
- (Exam Topic 3)
The PRIMARY objective of a risk identification process is to:

A. evaluate how risk conditions are managed.
B. determine threats and vulnerabilities.
C. estimate anticipated financial impact of risk conditions.
D. establish risk response options.

Answer: B

NEW QUESTION 236
- (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 239
- (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 244

- (Exam Topic 3)
A risk practitioner is developing a set of bottom-up IT risk scenarios. The MOST important time to involve business stakeholders is when:

A. updating the risk register
B. documenting the risk scenarios.
C. validating the risk scenarios
D. identifying risk mitigation controls.

Answer: C

NEW QUESTION 246
- (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 250
- (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 252
- (Exam Topic 3)
When formulating a social media policy lo address information leakage, which of the following is the MOST important concern to address?

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

Answer: A

NEW QUESTION 257
- (Exam Topic 3)
Which of the following should be the PRIMARY focus of an IT risk awareness program?

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

Answer: B

NEW QUESTION 262
- (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 263
- (Exam Topic 3)
Which of the following should be a risk practitioner's PRIMARY focus when tasked with ensuring organization records are being retained for a sufficient period of time to meet legal obligations?

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

Answer: B

NEW QUESTION 268
- (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 269
- (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 271
- (Exam Topic 3)
Which of We following is the MOST effective control to address the risk associated with compromising data privacy within the cloud?

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

Answer: D

NEW QUESTION 272
- (Exam Topic 3)
A deficient control has been identified which could result in great harm to an organization should a low frequency threat event occur. When communicating the associated risk to senior management the risk practitioner should explain:

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

Answer: A

NEW QUESTION 273
- (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 278
- (Exam Topic 4)
Which of the following situations presents the GREATEST challenge to creating a comprehensive IT risk profile of an organization?

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

Answer: D

NEW QUESTION 279
- (Exam Topic 4)
Which of the following is MOST important to ensure when reviewing an organization's risk register?

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

Answer: A

NEW QUESTION 284
- (Exam Topic 4)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

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

Answer: C

NEW QUESTION 287
- (Exam Topic 4)
Which of the following BEST balances the costs and benefits of managing IT risk*?

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

Answer: A

NEW QUESTION 289
- (Exam Topic 4)
Which of the following is MOST helpful in defining an early-warning threshold associated with insufficient network bandwidth''

A. Average bandwidth usage
B. Peak bandwidth usage
C. Total bandwidth usage
D. Bandwidth used during business hours

Answer: A

NEW QUESTION 293
- (Exam Topic 4)
An information security audit identified a risk resulting from the failure of an automated control Who is responsible for ensuring the risk register is updated accordingly?

A. The risk practitioner
B. The risk owner
C. The control owner
D. The audit manager

Answer: A

NEW QUESTION 297
- (Exam Topic 4)
Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?

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

Answer: C

NEW QUESTION 299
- (Exam Topic 4)
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 300
- (Exam Topic 4)
An organization has agreed to a 99% availability for its online services and will not accept availability that falls below 98.5%. This is an example of:

A. risk mitigation.

B. risk evaluation.
C. risk appetite.
D. risk tolerance.

Answer: C

NEW QUESTION 302
- (Exam Topic 4)
Which of the following is the BEST approach to mitigate the risk associated with a control deficiency?

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

Answer: C

NEW QUESTION 307
- (Exam Topic 4)
Who should be responsible (of evaluating the residual risk after a compensating control has been

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

Answer: D

NEW QUESTION 309
- (Exam Topic 4)
Which of the following has the GREATEST influence on an organization's risk appetite?

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

Answer: D

NEW QUESTION 311
- (Exam Topic 4)
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

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

Answer: D

NEW QUESTION 313
- (Exam Topic 4)
Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

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

Answer: B

NEW QUESTION 315
- (Exam Topic 4)
Which of the following would be a risk practitioner’s BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

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

Answer: A

NEW QUESTION 316
- (Exam Topic 4)

What is the PRIMARY reason an organization should include background checks on roles with elevated access to production as part of its hiring process?

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

Answer: C

NEW QUESTION 319
- (Exam Topic 4)
When implementing an IT risk management program, which of the following is the BEST time to evaluate current control effectiveness?

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

Answer: B

NEW QUESTION 321
- (Exam Topic 4)
Which of the following potential scenarios associated with the implementation of a new database technology presents the GREATEST risk to an organization?

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

Answer: B

NEW QUESTION 325
- (Exam Topic 4)
Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

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

Answer: A

NEW QUESTION 328
- (Exam Topic 4)
Following an acquisition, the acquiring company's risk practitioner has been asked to update the organization's IT risk profile What is the MOST important information to review from the acquired company to facilitate this task?

A. Internal and external audit reports
B. Risk disclosures in financial statements
C. Risk assessment and risk register
D. Business objectives and strategies

Answer: C

NEW QUESTION 332
- (Exam Topic 4)
Which of the following is the BEST key performance indicator (KPI) to measure how effectively risk management practices are embedded in the project management office (PMO)?

A. Percentage of projects with key risk accepted by the project steering committee
B. Reduction in risk policy noncompliance findings
C. Percentage of projects with developed controls on scope creep
D. Reduction in audits involving external risk consultants

Answer: C

NEW QUESTION 335
- (Exam Topic 4)
Which of the following is the MOST effective way 10 identify an application backdoor prior to implementation'?

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

Answer: B

NEW QUESTION 337
- (Exam Topic 4)
Which of the following BEST enables effective IT control implementation?

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

Answer: B

NEW QUESTION 340
- (Exam Topic 4)
Which of the following contributes MOST to the effective implementation of risk responses?

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

Answer: A

NEW QUESTION 343
- (Exam Topic 4)
The BEST indicator of the risk appetite of an organization is the

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

Answer: B

NEW QUESTION 344
- (Exam Topic 4)
An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

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

Answer: D

NEW QUESTION 349
- (Exam Topic 4)
Which stakeholder is MOST important to include when defining a risk profile during me selection process for a new third party application'?

A. The third-party risk manager
B. The application vendor
C. The business process owner
D. The information security manager

Answer: B

NEW QUESTION 350
- (Exam Topic 4)
A global organization has implemented an application that does not address all privacy requirements across multiple jurisdictions. Which of the following risk responses has the organization adopted with regard to privacy requirements?

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

Answer: A

NEW QUESTION 353
- (Exam Topic 4)
Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

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

Answer: C

NEW QUESTION 357
- (Exam Topic 4)
Which of the following is the MOST important outcome of a business impact analysis (BIA)?

A. Understanding and prioritization of critical processes
B. Completion of the business continuity plan (BCP)
C. Identification of regulatory consequences
D. Reduction of security and business continuity threats

Answer: A

NEW QUESTION 359
- (Exam Topic 4)
An organization's recovery team is attempting to recover critical data backups following a major flood in its data center. However, key team members do not know exactly what steps should be taken to address this crisis. Which of the following is the MOST likely cause of this situation?

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

Answer: A

NEW QUESTION 360
- (Exam Topic 4)
A control process has been implemented in response to a new regulatory requirement, but has significantly reduced productivity. Which of the following is the BEST way to resolve this concern?

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

Answer: C

NEW QUESTION 362
- (Exam Topic 4)
When reviewing the business continuity plan (BCP) of an online sales order system, a risk practitioner notices that the recovery time objective (RTO) has a shorter lime than what is defined in the disaster recovery plan (DRP). Which of the following is the BEST way for the risk practitioner to address this concern?

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

Answer: D

NEW QUESTION 365
- (Exam Topic 4)
Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

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

Answer: A

NEW QUESTION 369
- (Exam Topic 4)
Which of the following is MOST important for successful incident response?

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

Answer: D

NEW QUESTION 374
- (Exam Topic 4)
An organization is considering the adoption of an aggressive business strategy to achieve desired growth From a risk management perspective what should the

risk practitioner do NEXT?

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

Answer: A

NEW QUESTION 379
- (Exam Topic 4)
Which of the following is the BEST approach for selecting controls to minimize risk?

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

Answer: C

NEW QUESTION 381
- (Exam Topic 4)
Which of the following proposed benefits is MOST likely to influence senior management approval to reallocate budget for a new security initiative?

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

Answer: B

NEW QUESTION 385
- (Exam Topic 4)
Effective risk communication BEST benefits an organization by:

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

Answer: A

NEW QUESTION 386
- (Exam Topic 4)
An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

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

Answer: A

NEW QUESTION 388
- (Exam Topic 4)
Which of the following is the result of a realized risk scenario?

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

Answer: D

NEW QUESTION 390
- (Exam Topic 4)
A risk practitioner has established that a particular control is working as desired, but the annual cost of maintenance has increased and now exceeds the expected annual loss exposure. The result is that the control is:

A. mature
B. ineffective.
C. optimized.
D. inefficient.

Answer: B

NEW QUESTION 392
- (Exam Topic 4)
Which of the following is the MOST important step to ensure regulatory requirements are adequately addressed within an organization?

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

Answer: B

NEW QUESTION 397
- (Exam Topic 4)
Of the following, who is responsible for approval when a change in an application system is ready for release to production?

A. Information security officer
B. IT risk manager
C. Business owner
D. Chief risk officer (CRO)

Answer: C

NEW QUESTION 398
- (Exam Topic 4)
Who should be responsible for determining which stakeholders need to be involved in the development of a risk scenario?

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

Answer: B

NEW QUESTION 401
- (Exam Topic 4)
An organization is implementing robotic process automation (RPA) to streamline business processes. Given that implementation of this technology is expected to impact existing controls, which of the following is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 404
- (Exam Topic 4)
Which of the following would be of GREATEST concern regarding an organization's asset management?

A. Lack of a mature records management program
B. Lack of a dedicated asset management team
C. Decentralized asset lists
D. Incomplete asset inventory

Answer: D

NEW QUESTION 405
- (Exam Topic 4)
The MAIN purpose of selecting a risk response is to.

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

Answer: C

NEW QUESTION 407
- (Exam Topic 4)
What should be the PRIMARY consideration related to data privacy protection when there are plans for a business initiative to make use of personal information?

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

Answer: D

NEW QUESTION 411
- (Exam Topic 4)
Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

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

Answer: A

NEW QUESTION 415
- (Exam Topic 4)
Which of the following should be the PRIMARY input to determine risk tolerance?

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

Answer: C

NEW QUESTION 420
- (Exam Topic 4)
An organization recently implemented a machine learning-based solution to monitor IT usage and analyze user behavior in an effort to detect internal fraud. Which of the following is MOST likely to be reassessed as a result of this initiative?

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

Answer: A

NEW QUESTION 422
- (Exam Topic 4)
Which of the following should be a risk practitioner's NEXT step after learning of an incident that has affected a competitor?

A. Activate the incident response plan.
B. Implement compensating controls.
C. Update the risk register.
D. Develop risk scenarios.

Answer: A

NEW QUESTION 426
- (Exam Topic 4)
Which of the following should be the PRIMARY basis for prioritizing risk responses?

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

Answer: A

NEW QUESTION 429
- (Exam Topic 4)
Which of the following would BEST mitigate the ongoing risk associated with operating system (OS) vulnerabilities?

A. Temporarily mitigate the OS vulnerabilities
B. Document and implement a patching process
C. Evaluate permanent fixes such as patches and upgrades
D. Identify the vulnerabilities and applicable OS patches

Answer: B

NEW QUESTION 433
- (Exam Topic 4)
An internal audit report reveals that a legacy system is no longer supported Which of the following is the risk practitioner's MOST important action before recommending a risk response'

A. Review historical application down me and frequency

B. Assess the potential impact and cost of mitigation
C. identify other legacy systems within the organization
D. Explore the feasibility of replacing the legacy system

Answer: B

NEW QUESTION 437
- (Exam Topic 4)
Which of the following is the MOST important benefit of reporting risk assessment results to senior management?

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

Answer: D

NEW QUESTION 442
- (Exam Topic 4)
it was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern1?

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

Answer: C

NEW QUESTION 444
- (Exam Topic 4)
Which of the following is a risk practitioner's BEST course of action after identifying risk scenarios related to noncompliance with new industry regulations?

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

Answer: D

NEW QUESTION 448
- (Exam Topic 3)
Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

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

Answer: A

NEW QUESTION 453
- (Exam Topic 3)
Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

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

Answer: C

NEW QUESTION 455
- (Exam Topic 3)
Which of the following should be implemented to BEST mitigate the risk associated with infrastructure updates?

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

Answer: C

NEW QUESTION 460
- (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 464
- (Exam Topic 3)
To minimize the risk of a potential acquisition being exposed externally, an organization has selected a few key employees to be engaged in the due diligence process. A member of the due diligence team realizes a close acquaintance is a high-ranking IT professional at a subsidiary of the company about to be acquired. What is the BEST course of action for this team member?

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

Answer: B

NEW QUESTION 468
- (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 470
- (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 474
- (Exam Topic 3)
When an organization’s disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?

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

Answer: B

NEW QUESTION 477
- (Exam Topic 3)
Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

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

Answer: A

NEW QUESTION 478
- (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 479
- (Exam Topic 3)
Which of the following practices BEST mitigates risk related to enterprise-wide ethical decision making in a multi-national organization?

A. Customized regional training on local laws and regulations
B. Policies requiring central reporting of potential procedure exceptions
C. Ongoing awareness training to support a common risk culture
D. Zero-tolerance policies for risk taking by middle-level managers

Answer: A

NEW QUESTION 481
- (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 486
- (Exam Topic 3)
Senior management has asked a risk practitioner to develop technical risk scenarios related to a recently developed enterprise resource planning (ERP) system. These scenarios will be owned by the system manager. Which of the following would be the BEST method to use when developing the scenarios?

A. Cause-and-effect diagram
B. Delphi technique
C. Bottom-up approach
D. Top-down approach

Answer: A

NEW QUESTION 488
- (Exam Topic 3)
Which of the following is the BEST course of action to help reduce the probability of an incident recurring?

A. Perform a risk assessment.
B. Perform root cause analysis.
C. Initiate disciplinary action.
D. Update the incident response plan.

Answer: B

NEW QUESTION 493
- (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 496
- (Exam Topic 3)
Which of the following is the BEST indicator of an effective IT security awareness program?

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

Answer: A

NEW QUESTION 497
- (Exam Topic 3)
An organization automatically approves exceptions to security policies on a recurring basis. This practice is MOST likely the result of:

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

Answer:

D

NEW QUESTION 501
- (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 505
- (Exam Topic 3)
Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?

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

Answer: A

NEW QUESTION 510
- (Exam Topic 3)
A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

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

Answer: A

NEW QUESTION 511
- (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 515
- (Exam Topic 3)
Which of the following approaches would BEST help to identify relevant risk scenarios?

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

Answer: A

NEW QUESTION 517
- (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 522
- (Exam Topic 3)
A risk practitioner has become aware of production data being used in a test environment. Which of the following should be the practitioner's PRIMARY concern?

A. Sensitivity of the data

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

Answer: A

NEW QUESTION 526
- (Exam Topic 3)
The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

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

Answer: D

NEW QUESTION 527
- (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 530
- (Exam Topic 3)
Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

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

Answer: C

NEW QUESTION 533
- (Exam Topic 3)
An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

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

Answer: B

NEW QUESTION 537
- (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 539
- (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 543

- (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 544
- (Exam Topic 3)
Which of the following is the FIRST step when conducting a business impact analysis (BIA)?

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

Answer: A

NEW QUESTION 548
- (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 550
- (Exam Topic 3)
Which of the following MUST be updated to maintain an IT risk register?

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

Answer: C

NEW QUESTION 552
- (Exam Topic 3)
While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially Which of the following would be the BEST approach for the risk practitioner to take?

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

Answer: C

NEW QUESTION 555
- (Exam Topic 3)
Which of the following is the MOST effective way to integrate risk and compliance management?

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

Answer: A

NEW QUESTION 558
- (Exam Topic 3)
While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

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

Answer: D

NEW QUESTION 559
- (Exam Topic 3)
Which of the following is a KEY consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (Al) solutions into the organization?

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

Answer: B

NEW QUESTION 561
- (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 562
- (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 565
- (Exam Topic 2)
The purpose of requiring source code escrow in a contractual agreement is to:

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

Answer: B

NEW QUESTION 567
- (Exam Topic 2)
An organization is making significant changes to an application. At what point should the application risk profile be updated?

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

Answer: D

NEW QUESTION 571
- (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 573
- (Exam Topic 2)
A risk practitioner has just learned about new done FIRST?

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

D. Design IT risk mitigation plans.

Answer: B

NEW QUESTION 574
- (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 578
- (Exam Topic 2)
Which of the following key risk indicators (KRIs) is MOST effective for monitoring risk related to a bring your own device (BYOD) program?

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

Answer: D

NEW QUESTION 583
- (Exam Topic 2)
Which of The following is the MOST relevant information to include in a risk management strategy?

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

Answer: D

NEW QUESTION 584
- (Exam Topic 2)
Which of the following is MOST important when defining controls?

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

Answer: C

NEW QUESTION 589
- (Exam Topic 2)
When reporting risk assessment results to senior management, which of the following is MOST important to include to enable risk-based decision making?

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

Answer: A

NEW QUESTION 592
- (Exam Topic 2)
During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

A. Include the new risk scenario in the current risk assessment.
B. Postpone the risk assessment until controls are identified.
C. Request the risk scenario be removed from the register.
D. Exclude the new risk scenario from the current risk assessment

Answer: A

NEW QUESTION 594
- (Exam Topic 2)
Which of the following could BEST detect an in-house developer inserting malicious functions into a web-based application?

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

Answer: B

NEW QUESTION 596
- (Exam Topic 2)
The BEST way to test the operational effectiveness of a data backup procedure is to:

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

Answer: D

NEW QUESTION 599
- (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 600
- (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 602
- (Exam Topic 2)
Which of the following is the BEST way to detect zero-day malware on an end user's workstation?

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

Answer: C

NEW QUESTION 606
- (Exam Topic 2)
An IT organization is replacing the customer relationship management (CRM) system. Who should own the risk associated with customer data leakage caused by insufficient IT security controls for the new system?

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

Answer: B

NEW QUESTION 609
- (Exam Topic 2)
Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

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

Answer: C

NEW QUESTION 613

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

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

Answer: D

NEW QUESTION 617
- (Exam Topic 2)
Which of the following is the MOST important information to be communicated during security awareness training?

A. Management's expectations
B. Corporate risk profile
C. Recent security incidents
D. The current risk management capability

Answer: A

NEW QUESTION 620
- (Exam Topic 2)
A risk practitioner has learned that an effort to implement a risk mitigation action plan has stalled due to lack of funding. The risk practitioner should report that the associated risk has been:

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

Answer: B

NEW QUESTION 625
- (Exam Topic 2)
Which of the following BEST helps to balance the costs and benefits of managing IT risk?

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

Answer: A

NEW QUESTION 630
- (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 632
- (Exam Topic 2)
Which of the following would MOST likely cause a risk practitioner to reassess risk scenarios?

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

Answer: C

NEW QUESTION 634
- (Exam Topic 2)
Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

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

Answer: D

NEW QUESTION 637
- (Exam Topic 2)
What are the MOST important criteria to consider when developing a data classification scheme to facilitate risk assessment and the prioritization of risk mitigation activities?

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

Answer: C

NEW QUESTION 639
- (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 642
- (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 645
- (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 650
- (Exam Topic 2)
Which of the following is MOST critical to the design of relevant risk scenarios?

A. The scenarios are based on past incidents.
B. The scenarios are linked to probable organizational situations.
C. The scenarios are mapped to incident management capabilities.
D. The scenarios are aligned with risk management capabilities.

Answer: B

NEW QUESTION 654
- (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 657
- (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 659
- (Exam Topic 2)
The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

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

Answer: C

NEW QUESTION 662
- (Exam Topic 2)
A risk practitioner is reviewing the status of an action plan to mitigate an emerging IT risk and finds the risk level has increased. The BEST course of action would be to:

A. implement the planned controls and accept the remaining risk.
B. suspend the current action plan in order to reassess the risk.
C. revise the action plan to include additional mitigating controls.
D. evaluate whether selected controls are still appropriate.

Answer: D

NEW QUESTION 663
- (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 666
- (Exam Topic 2)
Which of the following is the MOST effective way to mitigate identified risk scenarios?

A. Assign ownership of the risk response plan
B. Provide awareness in early detection of risk.
C. Perform periodic audits on identified risk.
D. areas Document the risk tolerance of the organization.

Answer: A

NEW QUESTION 669
- (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 671
- (Exam Topic 2)
An organization is planning to outsource its payroll function to an external service provider Which of the following should be the MOST important consideration when selecting the provider?

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

Answer: C

NEW QUESTION 674
- (Exam Topic 2)
Which of the following can be used to assign a monetary value to risk?

A. Annual loss expectancy (ALE)

B. Business impact analysis
C. Cost-benefit analysis
D. Inherent vulnerabilities

Answer: A

NEW QUESTION 676
- (Exam Topic 2)
Which of the following would prompt changes in key risk indicator {KRI) thresholds?

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

Answer: B

NEW QUESTION 679
- (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 682
- (Exam Topic 2)
Which of the following should management consider when selecting a risk mitigation option?

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

Answer: B

NEW QUESTION 685
- (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 688
- (Exam Topic 2)
Which of The following will BEST communicate the importance of risk mitigation initiatives to senior management?

A. Business case
B. Balanced scorecard
C. Industry standards
D. Heat map

Answer: A

NEW QUESTION 689
- (Exam Topic 2)
Which of the following is the PRIMARY reason for an organization to ensure the risk register is updated regularly?

A. Risk assessment results are accessible to senior management and stakeholders.
B. Risk mitigation activities are managed and coordinated.
C. Key risk indicators (KRIs) are evaluated to validate they are still within the risk threshold.
D. Risk information is available to enable risk-based decisions.

Answer: D

NEW QUESTION 692
- (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 697
- (Exam Topic 2)
Which of the following is the BEST indicator of the effectiveness of a control monitoring program?

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

Answer: A

NEW QUESTION 700
- (Exam Topic 2)
To minimize risk in a software development project, when is the BEST time to conduct a risk analysis?

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

Answer: A

NEW QUESTION 703
- (Exam Topic 2)
When establishing leading indicators for the information security incident response process it is MOST important to consider the percentage of reported incidents:

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

Answer: C

NEW QUESTION 706
- (Exam Topic 2)
Which of the following is the BEST way to determine software license compliance?

A. List non-compliant systems in the risk register.
B. Conduct periodic compliance reviews.
C. Review whistlebtower reports of noncompliance.
D. Monitor user software download activity.

Answer: B

NEW QUESTION 709
- (Exam Topic 2)
Which of the following is the BEST way to identify changes in the risk profile of an organization?

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

Answer: D

NEW QUESTION 710
- (Exam Topic 2)
Which of the following would MOST likely result in updates to an IT risk appetite statement?

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

Answer: D

NEW QUESTION 715
- (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 718
- (Exam Topic 2)
A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

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

Answer: C

NEW QUESTION 723
- (Exam Topic 2)
A risk practitioner notices a trend of noncompliance with an IT-related control. Which of the following would BEST assist in making a recommendation to management?

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

Answer: A

NEW QUESTION 726
- (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 728
- (Exam Topic 2)
During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 730
- (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 731
- (Exam Topic 2)
Which of the following would BEST enable a risk practitioner to embed risk management within the organization?

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

D. Engage key stakeholders in risk management practices.

Answer: D

NEW QUESTION 735
- (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 740
- (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 745
- (Exam Topic 2)
Which of the following requirements is MOST important to include in an outsourcing contract to help ensure sensitive data stored with a service provider is secure?

A. A third-party assessment report of control environment effectiveness must be provided at least annually.
B. Incidents related to data toss must be reported to the organization immediately after they occur.
C. Risk assessment results must be provided to the organization at least annually.
D. A cyber insurance policy must be purchased to cover data loss events.

Answer: A

NEW QUESTION 749
- (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 750
- (Exam Topic 2)
During the control evaluation phase of a risk assessment, it is noted that multiple controls are ineffective. Which of the following should be the risk practitioner's FIRST course of action?

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

Answer: C

NEW QUESTION 754
- (Exam Topic 2)
Which of the following is MOST important to understand when developing key risk indicators (KRIs)?

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

Answer: B

NEW QUESTION 756
- (Exam Topic 2)
The PRIMARY purpose of vulnerability assessments is to:

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

Answer: D

NEW QUESTION 761
- (Exam Topic 2)
The risk appetite for an organization could be derived from which of the following?

A. Cost of controls
B. Annual loss expectancy (ALE)
C. Inherent risk
D. Residual risk

Answer: A

NEW QUESTION 762
- (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: C

NEW QUESTION 767
- (Exam Topic 2)
Which of the following is the GREATEST concern when an organization uses a managed security service provider as a firewall administrator?

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

Answer: B

NEW QUESTION 771
- (Exam Topic 2)
For no apparent reason, the time required to complete daily processing for a legacy application is approaching a risk threshold. Which of the following activities should be performed FIRST?

A. Temporarily increase the risk threshold.
B. Suspend processing to investigate the problem.
C. Initiate a feasibility study for a new application.
D. Conduct a root-cause analysis.

Answer: D

NEW QUESTION 772
- (Exam Topic 2)
An identified high probability risk scenario involving a critical, proprietary business function has an annualized cost of control higher than the annual loss expectancy. Which of the following is the BEST risk response?

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

Answer: B

NEW QUESTION 773
- (Exam Topic 2)
Which of the following would BEST help identify the owner for each risk scenario in a risk register?

A. Determining which departments contribute most to risk
B. Allocating responsibility for risk factors equally to asset owners
C. Mapping identified risk factors to specific business processes
D. Determining resource dependency of assets

Answer: C

NEW QUESTION 777
- (Exam Topic 2)
The BEST way to demonstrate alignment of the risk profile with business objectives is through:

A. risk scenarios.
B. risk tolerance.
C. risk policy.
D. risk appetite.

Answer: B

NEW QUESTION 780
- (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 785
- (Exam Topic 2)
Which of the following would be of GREATEST assistance when justifying investment in risk response strategies?

A. Total cost of ownership
B. Resource dependency analysis
C. Cost-benefit analysis
D. Business impact analysis

Answer: C

NEW QUESTION 790
- (Exam Topic 2)
An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

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

Answer: B

NEW QUESTION 792
- (Exam Topic 2)
Which of the following should be the PRIMARY recipient of reports showing the progress of a current IT risk mitigation project?

A. Senior management
B. Project manager
C. Project sponsor
D. IT risk manager

Answer: A

NEW QUESTION 795
- (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 798
- (Exam Topic 2)
An organization has completed a project to implement encryption on all databases that host customer data. Which of the following elements of the risk register should be updated the reflect this change?

A. Risk likelihood
B. Inherent risk
C. Risk appetite
D. Risk tolerance

Answer: B

NEW QUESTION 799
- (Exam Topic 2)
What should a risk practitioner do FIRST when vulnerability assessment results identify a weakness in an application?

A. Review regular control testing results.
B. Recommend a penetration test.
C. Assess the risk to determine mitigation needed.
D. Analyze key performance indicators (KPIs).

Answer: C

NEW QUESTION 800
- (Exam Topic 2)
Which of the following is the BEST method for identifying vulnerabilities?

A. Batch job failure monitoring
B. Periodic network scanning
C. Annual penetration testing
D. Risk assessments

Answer: C

NEW QUESTION 805
- (Exam Topic 2)
Which of the following methods is the BEST way to measure the effectiveness of automated information security controls prior to going live?

A. Testing in a non-production environment
B. Performing a security control review
C. Reviewing the security audit report
D. Conducting a risk assessment

Answer: A

NEW QUESTION 810
- (Exam Topic 2)
Which of the following is the MOST important data attribute of key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 811
- (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 816
- (Exam Topic 2)
To help ensure all applicable risk scenarios are incorporated into the risk register, it is MOST important to review the:

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

Answer: C

NEW QUESTION 819
- (Exam Topic 2)
Which of the following indicates an organization follows IT risk management best practice?

A. The risk register template uses an industry standard.
B. The risk register is regularly updated.
C. All fields in the risk register have been completed.

D. Controls are listed against risk entries in the register.

Answer: A

NEW QUESTION 824
- (Exam Topic 2)
The MOST significant benefit of using a consistent risk ranking methodology across an organization is that it enables:

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

Answer: B

NEW QUESTION 825
- (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 826
- (Exam Topic 2)
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?

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

Answer: A

NEW QUESTION 829
- (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 832
- (Exam Topic 2)
An organization has decided to implement an emerging technology and incorporate the new capabilities into its strategic business plan. Business operations for the technology will be outsourced. What will be the risk practitioner's PRIMARY role during the change?

A. Managing third-party risk
B. Developing risk scenarios
C. Managing the threat landscape
D. Updating risk appetite

Answer: B

NEW QUESTION 835
- (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 836
- (Exam Topic 2)
Following a review of a third-party vendor, it is MOST important for an organization to ensure:

A. results of the review are accurately reported to management.
B. identified findings are reviewed by the organization.
C. results of the review are validated by internal audit.
D. identified findings are approved by the vendor.

Answer: A

NEW QUESTION 839
- (Exam Topic 2)
Which of The following is the PRIMARY consideration when establishing an organization's risk management methodology?

A. Business context
B. Risk tolerance level
C. Resource requirements
D. Benchmarking information

Answer: A

NEW QUESTION 842
- (Exam Topic 2)
Which of the following is MOST helpful in verifying that the implementation of a risk mitigation control has been completed as intended?

A. An updated risk register
B. Risk assessment results
C. Technical control validation
D. Control testing results

Answer: D

NEW QUESTION 845
- (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 848
- (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 850
- (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 855
- (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 857

- (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 860
- (Exam Topic 2)
IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

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

Answer: D

NEW QUESTION 862
- (Exam Topic 2)
After mapping generic risk scenarios to organizational security policies, the NEXT course of action should be to:

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

Answer: B

NEW QUESTION 867
- (Exam Topic 2)
The MOST important reason to monitor key risk indicators (KRIs) is to help management:

A. identity early risk transfer strategies.
B. lessen the impact of realized risk.
C. analyze the chain of risk events.
D. identify the root cause of risk events.

Answer: C

NEW QUESTION 868
- (Exam Topic 2)
Which of the following is the PRIMARY reason to establish the root cause of an IT security incident?

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

Answer: D

NEW QUESTION 873
- (Exam Topic 2)
Which of the following should be of GREATEST concern to a risk practitioner when determining the effectiveness of IT controls?

A. Configuration updates do not follow formal change control.
B. Operational staff perform control self-assessments.
C. Controls are selected without a formal cost-benefit
D. analysis-Management reviews security policies once every two years.

Answer: A

NEW QUESTION 877
- (Exam Topic 2)
Which of the following is the MOST important consideration when identifying stakeholders to review risk scenarios developed by a risk analyst? The reviewers are:

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

Answer: D

NEW QUESTION 878
- (Exam Topic 2)
Which of the following presents the GREATEST challenge for an IT risk practitioner who wants to report on trends in historical IT risk levels?

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

Answer: A

NEW QUESTION 883
- (Exam Topic 2)
Once a risk owner has decided to implement a control to mitigate risk, it is MOST important to develop:

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

Answer: A

NEW QUESTION 886
- (Exam Topic 2)
Which of the following BEST indicates effective information security incident management?

A. Monthly trend of information security-related incidents
B. Average time to identify critical information security incidents
C. Frequency of information security incident response plan testing
D. Percentage of high risk security incidents

Answer: C

NEW QUESTION 888
- (Exam Topic 2)
A risk owner should be the person accountable for:

A. the risk management process
B. managing controls.
C. implementing actions.
D. the business process.

Answer: C

NEW QUESTION 889
- (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 894
- (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 899
- (Exam Topic 2)
Which of the following BEST reduces the probability of laptop theft?

A. Cable lock
B. Acceptable use policy
C. Data encryption
D. Asset tag with GPS

Answer: A

NEW QUESTION 903

- (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 905

......