

Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control



NEW QUESTION 1

- (Exam Topic 4)

When classifying and prioritizing risk responses, the areas to address FIRST are those with:

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

Answer: C

NEW QUESTION 2

- (Exam Topic 4)

A failed IT system upgrade project has resulted in the corruption of an organization's asset inventory database. Which of the following controls BEST mitigates the impact of this incident?

- A. Encryption
- B. Authentication
- C. Configuration
- D. Backups

Answer: D

NEW QUESTION 3

- (Exam Topic 4)

Which of the following is the BEST way to ensure data is properly sanitized while in cloud storage?

- A. Deleting the data from the file system
- B. Cryptographically scrambling the data
- C. Formatting the cloud storage at the block level
- D. Degaussing the cloud storage media

Answer: B

NEW QUESTION 4

- (Exam Topic 4)

Which of the following is the GREATEST benefit of having a mature enterprise architecture (EA) in place?

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

Answer: C

NEW QUESTION 5

- (Exam Topic 4)

Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 6

- (Exam Topic 4)

Which of 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-wide phishing simulations.
- C. Require training on the data handling policy.
- D. Require regular testing of the data breach response plan.

Answer: B

NEW QUESTION 7

- (Exam Topic 4)

Which of the following is the MOST important information to cover a business continuity awareness training 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 8

- (Exam Topic 4)

A poster has been displayed in a data center that reads. "Anyone caught taking photographs in the data center may be subject to disciplinary action." Which of the following control types has been implemented?

- A. Corrective
- B. Detective
- C. Deterrent
- D. Preventative

Answer: A

NEW QUESTION 9

- (Exam Topic 4)

Which of the following should be of MOST concern to a risk practitioner reviewing an organization risk register after the completion of a series of risk assessments?

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

Answer: A

NEW QUESTION 10

- (Exam Topic 4)

An organization is considering outsourcing user administration controls for a critical system. The potential vendor has offered to perform quarterly self-audits of its controls instead of having annual independent audits. Which of the following should be of GREATEST concern to the 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 11

- (Exam Topic 4)

Which of the following provides the MOST useful information for developing key risk indicators (KRIs)?

- A. Business impact analysis (BIA) results
- B. Risk scenario ownership
- C. Risk thresholds
- D. Possible causes of materialized risk

Answer: C

NEW QUESTION 15

- (Exam Topic 4)

Which of the following is the GREATEST benefit of using IT risk scenarios?

- A. They support compliance with regulations.
- B. They provide evidence of risk assessment.
- C. They facilitate communication of risk.
- D. They enable the use of key risk indicators (KRIs)

Answer: C

NEW QUESTION 16

- (Exam Topic 4)

Which of the following is PRIMARILY a risk management responsibility 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 18

- (Exam Topic 4)

Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

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

Answer: D

NEW QUESTION 22

- (Exam Topic 4)

A root cause analysis indicates a major service disruption due to a lack of competency of newly hired IT system administrators. Who should be accountable for resolving the situation?

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

Answer: C

NEW QUESTION 27

- (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 32

- (Exam Topic 4)

When establishing an enterprise IT risk management program, it is MOST important to:

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

Answer: D

NEW QUESTION 33

- (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 37

- (Exam Topic 4)

Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

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

Answer: A

NEW QUESTION 41

- (Exam Topic 4)

When is the BEST to identify risk associated with major project to determine a mitigation plan?

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

Answer: D

NEW QUESTION 42

- (Exam Topic 4)

Which of the following is MOST likely to introduce risk for financial institutions that use blockchain?

- A. Cost of implementation
- B. Implementation of unproven applications
- C. Disruption to business processes
- D. Increase in attack surface area

Answer: B

NEW QUESTION 43

- (Exam Topic 4)

Which of The following BEST represents the desired risk posture for an organization?

- A. Inherent risk is lower than risk tolerance.
- B. Operational risk is higher than risk tolerance.
- C. Accepted risk is higher than risk tolerance.
- D. Residual risk is lower than risk tolerance.

Answer: D

NEW QUESTION 46

- (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 51

- (Exam Topic 4)

Which of the following is the PRIMARY purpose of creating and documenting control procedures?

- A. To facilitate ongoing audit and control testing
- B. To help manage risk to acceptable tolerance levels
- C. To establish and maintain a control inventory
- D. To increase the likelihood of effective control operation

Answer: D

NEW QUESTION 53

- (Exam Topic 4)

Which of the following is the BEST method to maintain a common view of IT risk within an organization?

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

Answer: C

NEW QUESTION 55

- (Exam Topic 4)

Which of the following provides the BEST assurance of the effectiveness of vendor security controls?

- A. Review vendor control self-assessments (CSA).
- B. Review vendor service level agreement (SLA) metrics.
- C. Require independent control assessments.
- D. Obtain vendor references from existing customers.

Answer: C

NEW QUESTION 56

- (Exam Topic 3)

Which of the following BEST measures the impact of business interruptions caused by an IT service outage?

- A. Sustained financial loss
- B. Cost of remediation efforts
- C. Duration of service outage
- D. Average time to recovery

Answer: A

NEW QUESTION 58

- (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 63

- (Exam Topic 4)

A risk practitioner implemented a process to notify management of emergency changes that may not be approved. Which of the following is the BEST way to provide this information to management?

- A. Change logs
- B. Change management meeting minutes
- C. Key control indicators (KCI)s
- D. Key risk indicators (KRIs)

Answer: C

NEW QUESTION 66

- (Exam Topic 3)

An organization has implemented a preventive control to lock user accounts after three unsuccessful login attempts. This practice has been proven to be unproductive, and a change in the control threshold value has been recommended. Who should authorize changing this threshold?

- A. Risk owner
- B. IT security manager
- C. IT system owner
- D. Control owner

Answer: D

NEW QUESTION 71

- (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 72

- (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 76

- (Exam Topic 3)

An organization has initiated a project to launch an IT-based service to customers and take advantage of being the first to market. Which of the following should be of GREATEST concern to senior management?

- A. More time has been allotted for testing.
- B. The project is likely to deliver the product late.
- C. A new project manager is handling the project.

D. The cost of the project will exceed the allotted budget.

Answer: B

NEW QUESTION 81

- (Exam Topic 3)

Which of the following is MOST important to include in a risk assessment of an emerging technology?

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

Answer: D

NEW QUESTION 85

- (Exam Topic 3)

Which of the following controls are BEST strengthened by a clear organizational code of ethics?

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

Answer: B

NEW QUESTION 90

- (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 95

- (Exam Topic 3)

Which of the following is the MOST important objective of establishing an enterprise risk management (ERM) function within an organization?

- A. To have a unified approach to risk management across the organization
- B. To have a standard risk management process for complying with regulations
- C. To optimize risk management resources across the organization
- D. To ensure risk profiles are presented in a consistent format within the organization

Answer: A

NEW QUESTION 100

- (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 105

- (Exam Topic 3)

Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

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

Answer: B

NEW QUESTION 110

- (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 114

- (Exam Topic 3)

Which of the following will help ensure the elective decision-making of an IT risk management committee?

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

Answer: D

NEW QUESTION 119

- (Exam Topic 3)

A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

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

Answer: D

NEW QUESTION 122

- (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 126

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 129

- (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 130

- (Exam Topic 3)

From a risk management perspective, the PRIMARY objective of using maturity models is to enable:

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

Answer: C

NEW QUESTION 134

- (Exam Topic 3)

Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

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

Answer: C

NEW QUESTION 139

- (Exam Topic 3)

Which of the following is the PRIMARY benefit of using an entry in the risk register to track the aggregate risk associated with server failure?

- A. It provides a cost-benefit analysis on control options available for implementation.
- B. It provides a view on where controls should be applied to maximize the uptime of servers.
- C. It provides historical information about the impact of individual servers malfunctioning.
- D. It provides a comprehensive view of the impact should the servers simultaneously fail.

Answer: D

NEW QUESTION 144

- (Exam Topic 3)

Risk acceptance of an exception to a security control would MOST likely be justified when:

- A. automation cannot be applied to the control
- B. business benefits exceed the loss exposure.
- C. the end-user license agreement has expired.
- D. the control is difficult to enforce in practice.

Answer: B

NEW QUESTION 147

- (Exam Topic 3)

Which of the following BEST indicates the condition of a risk management program?

- A. Number of risk register entries
- B. Number of controls
- C. Level of financial support
- D. Amount of residual risk

Answer: D

NEW QUESTION 150

- (Exam Topic 3)

Which of the following represents a vulnerability?

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

Answer: C

NEW QUESTION 151

- (Exam Topic 3)

An organization has been notified that a disgruntled, terminated IT administrator has tried to break into the corporate network. Which of the following discoveries should be of GREATEST concern to the organization?

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

Answer: A

NEW QUESTION 156

- (Exam Topic 3)

Which of the following is MOST important for an organization to update following a change in legislation requiring notification to individuals impacted by data breaches?

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

Answer: C

NEW QUESTION 161

- (Exam Topic 3)

Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?

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

Answer: B

NEW QUESTION 163

- (Exam Topic 3)

Which of the following is the BEST evidence that a user account has been properly authorized?

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

Answer: C

NEW QUESTION 164

- (Exam Topic 3)

The MOST important objective of information security controls is to:

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

Answer: C

NEW QUESTION 165

- (Exam Topic 3)

Which of the following should be of GREATEST concern to a risk practitioner reviewing the implementation of an emerging technology?

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

Answer: B

NEW QUESTION 170

- (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 175

- (Exam Topic 3)

An internal audit report reveals that not all IT application databases have encryption in place. Which of the following information would be MOST important for assessing the risk impact?

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

Answer: B

NEW QUESTION 179

- (Exam Topic 3)

Who should have the authority to approve an exception to a control?

- A. information security manager
- B. Control owner
- C. Risk owner
- D. Risk manager

Answer:

C

NEW QUESTION 184

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 185

- (Exam Topic 3)

Which of the following BEST indicates whether security awareness training is effective?

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

Answer: B

NEW QUESTION 189

- (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 193

- (Exam Topic 3)

Which of the following BEST indicates how well a web infrastructure protects critical information from an attacker?

- A. Failed login attempts
- B. Simulating a denial of service attack
- C. Absence of IT audit findings
- D. Penetration test

Answer: D

NEW QUESTION 197

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 201

- (Exam Topic 3)

A risk practitioner identifies a database application that has been developed and implemented by the business independently of IT. Which of the following is the BEST course of action?

- A. Escalate the concern to senior management.
- B. Document the reasons for the exception.
- C. Include the application in IT risk assessments.
- D. Propose that the application be transferred to IT.

Answer: B

NEW QUESTION 204

- (Exam Topic 3)

The BEST way to obtain senior management support for investment in a control implementation would be to articulate the reduction in:

- A. detected incidents.

- B. residual risk.
- C. vulnerabilities.
- D. inherent risk.

Answer: D

NEW QUESTION 208

- (Exam Topic 3)

Which of the following is the PRIMARY reason to use key control indicators (KCI) 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 211

- (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 212

- (Exam Topic 3)

Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

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

Answer: B

NEW QUESTION 215

- (Exam Topic 3)

Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

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

Answer: A

NEW QUESTION 219

- (Exam Topic 3)

A risk practitioner is preparing a report to communicate changes in the risk and control environment. The BEST way to engage stakeholder attention is to:

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

Answer: B

NEW QUESTION 220

- (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 225

- (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 229

- (Exam Topic 3)

The risk associated with an asset after controls are applied can be expressed as:

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

Answer: C

NEW QUESTION 230

- (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 232

- (Exam Topic 3)

Which of the following will be MOST effective in uniquely identifying the originator of electronic transactions?

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

Answer: A

NEW QUESTION 236

- (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 240

- (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 242

- (Exam Topic 3)

An organization outsources the processing of us payroll data A risk practitioner identifies a control weakness at the third party trial exposes the payroll data. Who should own this risk?

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

Answer: B

NEW QUESTION 243

- (Exam Topic 3)

When evaluating enterprise IT risk management it is MOST important to:

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

Answer: B

NEW QUESTION 248

- (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 253

- (Exam Topic 3)

Which of the following is a risk practitioner's BEST recommendation to address an organization's need to secure multiple systems with limited IT resources?

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

Answer: C

NEW QUESTION 258

- (Exam Topic 3)

Which of the following is the MOST important component in a risk treatment plan?

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

Answer: D

NEW QUESTION 263

- (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 264

- (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 268

- (Exam Topic 3)

Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?

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

Answer: C

NEW QUESTION 270

- (Exam Topic 3)

Which of the following is MOST important to compare against the corporate risk profile?

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

Answer: D

NEW QUESTION 272

- (Exam Topic 3)

Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

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

Answer: A

NEW QUESTION 276

- (Exam Topic 3)

When formulating a social media policy to 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 279

- (Exam Topic 3)

Which of the following issues should be of GREATEST concern when evaluating existing controls during a risk assessment?

- A. A high number of approved exceptions exist with compensating controls.
- B. Successive assessments have the same recurring vulnerabilities.
- C. Redundant compensating controls are in place.
- D. Asset custodians are responsible for defining controls instead of asset owners.

Answer: B

NEW QUESTION 282

- (Exam Topic 3)

To communicate the risk associated with IT in business terms, which of the following MUST be defined?

- A. Compliance objectives
- B. Risk appetite of the organization
- C. Organizational objectives
- D. Inherent and residual risk

Answer: C

NEW QUESTION 286

- (Exam Topic 3)

Which of the following approaches BEST identifies information systems control deficiencies?

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

Answer: C

NEW QUESTION 290

- (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 294

- (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 298

- (Exam Topic 3)

Which of the following is the BEST way to quantify the likelihood of risk materialization?

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

Answer: D

NEW QUESTION 301

- (Exam Topic 3)

Days before the realization of an acquisition, a data breach is discovered at the company to be acquired. For the accruing organization, this situation represents which of the following?

- A. Threat event
- B. Inherent risk
- C. Risk event
- D. Security incident

Answer: B

NEW QUESTION 305

- (Exam Topic 3)

Which of the 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 provider to 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 307

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 308

- (Exam Topic 3)

An organization is implementing internet of Things (IoT) technology to control temperature and lighting in its headquarters. Which of the following should be of GREATEST concern?

- A. Insufficient network isolation
- B. impact on network performance
- C. insecure data transmission protocols
- D. Lack of interoperability between sensors

Answer: D

NEW QUESTION 312

- (Exam Topic 4)

The objective of aligning mitigating controls to risk appetite is to ensure that:

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

Answer: D

NEW QUESTION 316

- (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 320

- (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 324

- (Exam Topic 4)

Senior management is deciding whether to share confidential data with the organization's business partners. The BEST course of action for a risk practitioner would be to submit a report to senior management containing the:

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

Answer: A

NEW QUESTION 326

- (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 329

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 332

- (Exam Topic 4)

Which of the following is the BEST way to ensure adequate resources will be allocated to manage identified risk?

- A. Prioritizing risk within each business unit
- B. Reviewing risk ranking methodology
- C. Promoting an organizational culture of risk awareness
- D. Assigning risk ownership to appropriate roles

Answer: D

NEW QUESTION 337

- (Exam Topic 4)

Which risk response strategy could management apply to both positive and negative risk that has been identified?

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

Answer: B

NEW QUESTION 338

- (Exam Topic 4)

Which of the following is the BEST way for a risk practitioner to present an annual risk management update to the board"

- A. A summary of risk response plans with validation results
- B. A report with control environment assessment results
- C. A dashboard summarizing key risk indicators (KRIs)
- D. A summary of IT risk scenarios with business cases

Answer: C

NEW QUESTION 343

- (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 346

- (Exam Topic 4)

Which of the following activities BEST facilitates effective risk management throughout the organization?

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

Answer: B

NEW QUESTION 351

- (Exam Topic 4)

Which of the following sources is MOST relevant to reference when updating security awareness training materials?

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

Answer: B

NEW QUESTION 355

- (Exam Topic 4)

When of the following standard operating procedure (SOP) statements BEST illustrates appropriate risk register maintenance?

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

Answer: C

NEW QUESTION 357

- (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 359

- (Exam Topic 4)

When performing a risk assessment of a new service to support a core business process, which of the following should be done FIRST to ensure continuity of operations?

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

Answer: B

NEW QUESTION 363

- (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 368

- (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 370

- (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 374

- (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 376

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 377

- (Exam Topic 4)

As part of business continuity planning, which of the following is MOST important to include in a business impact analysis (BIA)?

- A. An assessment of threats to the organization
- B. An assessment of recovery scenarios

- C. industry standard framework
- D. Documentation of testing procedures

Answer: A

NEW QUESTION 382

- (Exam Topic 4)

A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?

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

Answer: D

NEW QUESTION 387

- (Exam Topic 4)

Which of the following should be used as the PRIMARY basis for evaluating the state of an organization's cloud computing environment against leading practices?

- A. The cloud environment's capability maturity model
- B. The cloud environment's risk register
- C. The cloud computing architecture
- D. The organization's strategic plans for cloud computing

Answer: A

NEW QUESTION 390

- (Exam Topic 4)

An organization has operations in a location that regularly experiences severe weather events. Which of the following would BEST help to mitigate the risk to operations?

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

Answer: D

NEW QUESTION 391

- (Exam Topic 4)

One of an organization's key IT systems cannot be patched because the patches interfere with critical business application functionalities. Which of the following would be the risk practitioner's BEST recommendation?

- A. Additional mitigating controls should be identified.
- B. The system should not be used until the application is changed
- C. The organization's IT risk appetite should be adjusted.
- D. The associated IT risk should be accepted by management.

Answer: A

NEW QUESTION 396

- (Exam Topic 4)

Which of the following is the MAIN purpose of monitoring risk?

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

Answer: A

NEW QUESTION 400

- (Exam Topic 4)

Which of the following would BEST mitigate an identified risk scenario?

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

Answer: C

NEW QUESTION 401

- (Exam Topic 4)

To define the risk management strategy which of the following MUST be set by the board of directors?

- A. Operational strategies
- B. Risk governance
- C. Annualized loss expectancy (ALE)
- D. Risk appetite

Answer: B

NEW QUESTION 404

- (Exam Topic 4)

An organization wants to launch a campaign to advertise a new product Using data analytics, the campaign can be targeted to reach potential customers. Which of the following should be of GREATEST concern to the risk practitioner?

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

Answer: D

NEW QUESTION 409

- (Exam Topic 4)

Which of the blowing is MOST important when implementing an organization s security policy?

- A. Obtaining management support
- B. Benchmarking against industry standards
- C. Assessing compliance requirements
- D. Identifying threats and vulnerabilities

Answer: A

NEW QUESTION 413

- (Exam Topic 4)

When documenting a risk response, which of the following provides the STRONGEST evidence to support the decision?

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

Answer: C

NEW QUESTION 417

- (Exam Topic 4)

Which of the following s MOST likely to deter an employee from engaging in inappropriate use of company owned IT systems?

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

Answer: D

NEW QUESTION 422

- (Exam Topic 4)

Which of the following is MOST helpful in identifying loss magnitude during risk analysis of a new system?

- A. Recovery time objective (RTO)
- B. Cost-benefit analysis
- C. Business impact analysis (BIA)
- D. Cyber insurance coverage

Answer: C

NEW QUESTION 424

- (Exam Topic 4)

Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

- A. KRIs provide an early warning that a risk threshold is about to be reached.
- B. KRIs signal that a change in the control environment has occurred.
- C. KRIs provide a basis to set the risk appetite for an organization.
- D. KRIs assist in the preparation of the organization's risk profile.

Answer: A

NEW QUESTION 428

- (Exam Topic 4)

Which of the following should be considered FIRST when creating a comprehensive IT risk register?

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

Answer: C

NEW QUESTION 432

- (Exam Topic 4)

An organization has experienced a cyber attack that exposed customer personally identifiable information (PII) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

- A. Security control owners based on control failures
- B. Cyber risk remediation plan owners
- C. Risk owners based on risk impact
- D. Enterprise risk management (ERM) team

Answer: C

NEW QUESTION 435

- (Exam Topic 4)

Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

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

Answer: B

NEW QUESTION 436

- (Exam Topic 4)

Which of the following is the GREATEST benefit of centralizing IT systems?

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

Answer: C

NEW QUESTION 439

- (Exam Topic 4)

Which of the following is the BEST way to help ensure risk will be managed properly after a business process has been re-engineered?

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

Answer: A

NEW QUESTION 440

- (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 445

- (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 449

- (Exam Topic 4)

A risk practitioner is reviewing accountability assignments for data risk in the risk register. Which of the following would pose the GREATEST concern?

- A. The risk owner is not the control owner for associated data controls.
- B. The risk owner is in a business unit and does not report through the IT department.
- C. The risk owner is listed as the department responsible for decision making.
- D. The risk owner is a staff member rather than a department manager.

Answer: C

NEW QUESTION 451

- (Exam Topic 4)

The cost of maintaining a control has grown to exceed the potential loss. Which of the following BEST describes this situation?

- A. Insufficient risk tolerance
- B. Optimized control management
- C. Effective risk management
- D. Over-controlled environment

Answer: B

NEW QUESTION 455

- (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 460

- (Exam Topic 4)

Which of the following is the BEST way to protect sensitive data from administrators within a public cloud?

- A. Use an encrypted tunnel to connect to the cloud.
- B. Encrypt the data in the cloud database.
- C. Encrypt physical hard drives within the cloud.
- D. Encrypt data before it leaves the organization.

Answer: D

NEW QUESTION 465

- (Exam Topic 4)

Which of the following provides the MOST reliable evidence of a control's effectiveness?

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

Answer: D

NEW QUESTION 467

- (Exam Topic 4)

Which of the following is the BEST course of action when an organization wants to reduce likelihood in order to reduce a risk level?

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

Answer: B

NEW QUESTION 470

- (Exam Topic 4)

Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

- A. Internal auditor
- B. Asset owner
- C. Finance manager

D. Control owner

Answer: B

NEW QUESTION 475

- (Exam Topic 4)

Which key performance efficiency (KPI) BEST measures the effectiveness of an organization's disaster recovery program?

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

Answer: D

NEW QUESTION 477

- (Exam Topic 4)

Which of the following would be the GREATEST concern for an IT risk practitioner when an employee....

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

Answer: B

NEW QUESTION 478

- (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 479

- (Exam Topic 4)

Which of the following is the MOST effective way for a large and diversified organization to minimize risk associated with unauthorized software on company devices?

- A. Scan endpoints for applications not included in the asset inventory.
- B. Prohibit the use of cloud-based virtual desktop software.
- C. Conduct frequent reviews of software licenses.
- D. Perform frequent internal audits of enterprise IT infrastructure.

Answer: A

NEW QUESTION 482

- (Exam Topic 4)

An IT risk threat analysis is BEST used to establish

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

Answer: A

NEW QUESTION 487

- (Exam Topic 4)

After the implementation of Internet of Things (IoT) devices, new risk scenarios were identified. What is the PRIMARY reason to report this information to risk owners?

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

Answer: D

NEW QUESTION 489

- (Exam Topic 4)

Which organization is implementing a project to automate the purchasing process, including the modification of approval controls. Which of the following tasks is likely

responsibility of the risk practitioner*?

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

Answer: B

NEW QUESTION 490

- (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 492

- (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 494

- (Exam Topic 4)

Which of the following would MOST effectively reduce risk associated with an increase of online transactions on a retailer website?

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

Answer: C

NEW QUESTION 496

- (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 500

- (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 502

- (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 506

- (Exam Topic 3)

A risk practitioner has discovered a deficiency in a critical system that cannot be patched. Which of the following should be the risk practitioner's FIRST course of action?

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

Answer: C

NEW QUESTION 509

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 513

- (Exam Topic 3)

After a high-profile systems breach at an organization's key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:

Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

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

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

Answer: A

NEW QUESTION 516

- (Exam Topic 3)

Which of the following would BEST mitigate the risk associated with reputational damage from inappropriate use of social media sites by employees?

- A. Validating employee social media accounts and passwords
- B. Monitoring Internet usage on employee workstations
- C. Disabling social media access from the organization's technology
- D. Implementing training and awareness programs

Answer: D

NEW QUESTION 518

- (Exam Topic 3)

Which of the following describes the relationship between Key risk indicators (KRIs) and key control indicators (KCIs)?

- A. KCIs are independent from KRIs.
- B. KCIs and KRIs help in determining risk appetite.
- C. KCIs are defined using data from KRIs.
- D. KCIs provide input for KRIs.

Answer: D

NEW QUESTION 521

- (Exam Topic 3)

Which of the following should be the PRIMARY focus of a risk owner once a decision is made to mitigate a risk?

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

Answer: C

NEW QUESTION 526

- (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 528

- (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 532

- (Exam Topic 3)

An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

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

Answer: D

NEW QUESTION 537

- (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 542

- (Exam Topic 3)

Of the following, who is accountable for ensuring the effectiveness of a control to mitigate risk?

- A. Control owner
- B. Risk manager
- C. Control operator
- D. Risk treatment owner

Answer: A

NEW QUESTION 547

- (Exam Topic 3)

After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?

- A. Obtain industry benchmarks related to the specific risk.
- B. Provide justification for the lower risk rating.
- C. Notify the business at the next risk briefing.
- D. Reopen the risk issue and complete a full assessment.

Answer: B

NEW QUESTION 548

- (Exam Topic 3)

Which of the following is the FIRST step in risk assessment?

- A. Review risk governance

- B. Asset identification
- C. Identify risk factors
- D. Inherent risk identification

Answer: B

NEW QUESTION 553

- (Exam Topic 3)

Which of the following provides the BEST measurement of an organization's risk management maturity level?

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

Answer: C

NEW QUESTION 557

- (Exam Topic 3)

An organization's IT infrastructure is running end-of-life software that is not allowed without exception approval. Which of the following would provide the MOST helpful information to justify investing in updated software?

- A. The balanced scorecard
- B. A cost-benefit analysis
- C. The risk management frameworkD, A roadmap of IT strategic planning

Answer: B

NEW QUESTION 560

- (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 564

- (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 566

- (Exam Topic 3)

The PRIMARY purpose of IT control status reporting is to:

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

Answer: A

NEW QUESTION 567

- (Exam Topic 3)

Which of the following poses the GREATEST risk to an organization's operations during a major it transformation?

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

Answer: D

NEW QUESTION 570

- (Exam Topic 3)

The acceptance of control costs that exceed risk exposure MOST likely demonstrates:

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

Answer: C

NEW QUESTION 574

- (Exam Topic 3)

Which of the following is the GREATEST benefit to an organization when updates to the risk register are made promptly after the completion of a risk assessment?

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

Answer: B

NEW QUESTION 575

- (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 577

- (Exam Topic 3)

Which of the following will BEST help in communicating strategic risk priorities?

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

Answer: A

NEW QUESTION 578

- (Exam Topic 3)

Which of the following is the PRIMARY reason to adopt key control indicators (KCI)s in the risk monitoring and reporting process?

- A. To provide data for establishing the risk profile
- B. To provide assurance of adherence to risk management policies
- C. To provide measurements on the potential for risk to occur
- D. To provide assessments of mitigation effectiveness

Answer: D

NEW QUESTION 582

- (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 583

- (Exam Topic 3)

Which of the following is the BEST way for an organization to enable risk treatment decisions?

- A. Allocate sufficient funds for risk remediation.
- B. Promote risk and security awareness.
- C. Establish clear accountability for risk.
- D. Develop comprehensive policies and standards.

Answer: C

NEW QUESTION 587

- (Exam Topic 3)

Which of the following is the MOST common concern associated with outsourcing to a service provider?

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

Answer: C

NEW QUESTION 592

- (Exam Topic 3)

In an organization that allows employee use of social media accounts for work purposes, which of the following is the BEST way to protect company sensitive information from being exposed?

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

Answer: B

NEW QUESTION 595

- (Exam Topic 3)

Which of the following is MOST helpful to mitigate the risk associated with an application under development not meeting business objectives?

- A. Identifying tweets that may compromise enterprise architecture (EA)
- B. Including diverse Business scenarios in user acceptance testing (UAT)
- C. Performing risk assessments during the business case development stage
- D. Including key stakeholders in review of user requirements

Answer: D

NEW QUESTION 600

- (Exam Topic 3)

During an internal IT audit, an active network account belonging to a former employee was identified. Which of the following is the BEST way to prevent future occurrences?

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

Answer: A

NEW QUESTION 603

- (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 608

- (Exam Topic 3)

For a large software development project, risk assessments are MOST effective when performed:

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

Answer: C

NEW QUESTION 609

- (Exam Topic 3)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an antivirus program?

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

Answer: A

NEW QUESTION 612

- (Exam Topic 3)

An organization is implementing encryption for data at rest to reduce the risk associated with unauthorized access. Which of the following **MUST** be considered to assess the residual risk?

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

Answer: D

NEW QUESTION 615

- (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 619

- (Exam Topic 3)

Which of the following presents the **GREATEST** risk to change control in business application development over the complete life cycle?

- A. Emphasis on multiple application testing cycles
- B. Lack of an integrated development environment (IDE) tool
- C. Introduction of requirements that have not been approved
- D. Bypassing quality requirements before go-live

Answer: C

NEW QUESTION 623

- (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 625

- (Exam Topic 3)

Which of the following is a **KEY** consideration for a risk practitioner to communicate to senior management evaluating the introduction of artificial intelligence (AI) solutions into the organization?

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

Answer: B

NEW QUESTION 627

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 632

- (Exam Topic 2)

Quantifying the value of a single asset helps the organization to understand the:

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

Answer: B

NEW QUESTION 635

- (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 637

- (Exam Topic 2)

Which of the following is a crucial component of a key risk indicator (KRI) to ensure appropriate action is taken to mitigate risk?

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

Answer: D

NEW QUESTION 642

- (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 643

- (Exam Topic 2)

Which of the following is the MOST important consideration when selecting either a qualitative or quantitative risk analysis?

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

Answer: D

NEW QUESTION 647

- (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 650

- (Exam Topic 2)

Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?

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

Answer: D

NEW QUESTION 651

- (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 656

- (Exam Topic 2)

Which of the following statements in an organization's current risk profile report is cause for further action by senior management?

- A. Key performance indicator (KPI) trend data is incomplete.
- B. New key risk indicators (KRIs) have been established.
- C. Key performance indicators (KPIs) are outside of targets.
- D. Key risk indicators (KRIs) are lagging.

Answer: B

NEW QUESTION 659

- (Exam Topic 2)

Which of the following resources is MOST helpful when creating a manageable set of IT risk scenarios?

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

Answer: B

NEW QUESTION 664

- (Exam Topic 2)

Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?

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

Answer: A

NEW QUESTION 666

- (Exam Topic 2)

Which of the following conditions presents the GREATEST risk to an application?

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

Answer: D

NEW QUESTION 667

- (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 671

- (Exam Topic 2)

An organization is considering modifying its system to enable acceptance of credit card payments. To reduce the risk of data exposure, which of the following should the organization do FIRST?

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

Answer: A

NEW QUESTION 672

- (Exam Topic 2)

Which of the following is MOST essential for an effective change control environment?

- A. Business management approval of change requests
- B. Separation of development and production environments
- C. Requirement of an implementation rollback plan
- D. IT management review of implemented changes

Answer: A

NEW QUESTION 677

- (Exam Topic 2)

Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is aligned to business requirements?

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

Answer: C

NEW QUESTION 679

- (Exam Topic 2)

An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

- A. External resources may need to be involved.
- B. Data privacy regulations may be violated.
- C. Recovery costs may increase significantly.
- D. Service interruptions may be longer than anticipated.

Answer: D

NEW QUESTION 684

- (Exam Topic 2)

A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

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

Answer: A

NEW QUESTION 686

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?

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

Answer: D

NEW QUESTION 687

- (Exam Topic 2)

Which of the following should be the PRIMARY focus of an independent review of a risk management process?

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

Answer: B

NEW QUESTION 691

- (Exam Topic 2)

The FIRST task when developing a business continuity plan should be to:

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

Answer: B

NEW QUESTION 695

- (Exam Topic 2)

The GREATEST concern when maintaining a risk register is that:

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

Answer: D

NEW QUESTION 699

- (Exam Topic 2)

Which of the following would be a weakness in procedures for controlling the migration of changes to production libraries?

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

Answer: A

NEW QUESTION 702

- (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 707

- (Exam Topic 2)

Which of the following can be interpreted from a single data point on a risk heat map?

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

Answer: B

NEW QUESTION 711

- (Exam Topic 2)

A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

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

Answer: C

NEW QUESTION 713

- (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 717

- (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 718

- (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 719

- (Exam Topic 2)

A new policy has been published to forbid copying of data onto removable media. Which type of control has been implemented?

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

Answer: C

NEW QUESTION 722

- (Exam Topic 2)

Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?

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

Answer: A

NEW QUESTION 727

- (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 731

- (Exam Topic 2)

Mitigating technology risk to acceptable levels should be based PRIMARILY upon:

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

Answer: C

NEW QUESTION 736

- (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 739

- (Exam Topic 2)

Which of the following is the BEST way for a risk practitioner to verify that management has addressed control issues identified during a previous external audit?

- A. Interview control owners.
- B. Observe the control enhancements in operation.

- C. Inspect external audit documentation.
- D. Review management's detailed action plans.

Answer: B

NEW QUESTION 743

- (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 747

- (Exam Topic 2)

Which of the following would be MOST beneficial as a key risk indicator (KRI)?

- A. Current capital allocation reserves
- B. Negative security return on investment (ROI)
- C. Project cost variances
- D. Annualized loss projections

Answer: D

NEW QUESTION 751

- (Exam Topic 2)

The risk associated with a high-risk vulnerability in an application is owned by the:

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

Answer: B

NEW QUESTION 753

- (Exam Topic 2)

Which of the following should a risk practitioner do FIRST when an organization decides to use a cloud service?

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

Answer: D

NEW QUESTION 755

- (Exam Topic 2)

A risk practitioner has observed that risk owners have approved a high number of exceptions to the information security policy. Which of the following should be the risk practitioner's GREATEST concern?

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

Answer: D

NEW QUESTION 760

- (Exam Topic 2)

The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:

- A. rectify errors in results of KRIs.
- B. detect changes in the risk profile.
- C. reduce costs of risk mitigation controls.
- D. continually improve risk assessments.

Answer: B

NEW QUESTION 763

- (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 764

- (Exam Topic 2)

Which of the following is the MOST important consideration when performing a risk assessment of a fire suppression system within a data center?

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

Answer: C

NEW QUESTION 766

- (Exam Topic 2)

Which of the following is the MOST important input when developing risk scenarios?

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

Answer: B

NEW QUESTION 769

- (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 770

- (Exam Topic 2)

The maturity of an IT risk management program is MOST influenced by:

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

Answer: A

NEW QUESTION 773

- (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 778

- (Exam Topic 2)

Which of the following is the MOST important reason to create risk scenarios?

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

Answer: A

NEW QUESTION 782

- (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 783

- (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 788

- (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 793

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 795

- (Exam Topic 2)

Which of the following is MOST helpful in determining the effectiveness of an organization's IT risk mitigation efforts?

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

Answer: D

NEW QUESTION 800

- (Exam Topic 2)

Which of the following activities is PRIMARILY the responsibility of senior management?

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

Answer: C

NEW QUESTION 802

- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to consider when evaluating plans for changes to IT services?

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

Answer: B

NEW QUESTION 806

- (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 810

- (Exam Topic 2)

An organization's HR department has implemented a policy requiring staff members to take a minimum of five consecutive days leave per year to mitigate the risk of malicious insider activities. Which of the following is the BEST key performance indicator (KPI) of the effectiveness of this policy?

- A. Number of malicious activities occurring during staff members leave
- B. Percentage of staff members seeking exception to the policy
- C. Percentage of staff members taking leave according to the policy
- D. Financial loss incurred due to malicious activities during staff members' leave

Answer: B

NEW QUESTION 813

- (Exam Topic 2)

Which of the following provides The MOST useful information when determining a risk management program's maturity level?

- A. Risk assessment results
- B. A recently reviewed risk register
- C. Key performance indicators (KPIs)
- D. The organization's risk framework

Answer: A

NEW QUESTION 814

- (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 818

- (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 820

- (Exam Topic 2)

An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

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

Answer: B

NEW QUESTION 824

- (Exam Topic 2)

An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:

- A. identifying risk scenarios.
- B. determining the risk strategy.

- C. calculating impact and likelihood.
- D. completing the controls catalog.

Answer: A

NEW QUESTION 825

- (Exam Topic 2)

A risk practitioner observes that the fraud detection controls in an online payment system do not perform as expected. Which of the following will MOST likely change as a result?

- A. Impact
- B. Residual risk
- C. Inherent risk
- D. Risk appetite

Answer: B

NEW QUESTION 827

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 830

- (Exam Topic 2)

Who is MOST likely to be responsible for the coordination between the IT risk strategy and the business risk strategy?

- A. Chief financial officer
- B. Information security director
- C. Internal audit director
- D. Chief information officer

Answer: B

NEW QUESTION 835

- (Exam Topic 2)

A bank has outsourced its statement printing function to an external service provider. Which of the following is the MOST critical requirement to include in the contract?

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

Answer: D

NEW QUESTION 838

- (Exam Topic 2)

Which of the following activities should be performed FIRST when establishing IT risk management processes?

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

Answer: D

NEW QUESTION 841

- (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 844

- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to consider when determining the control requirements for data privacy arising from emerging technologies?

- A. internal audit recommendations
- B. Laws and regulations
- C. Policies and procedures
- D. Standards and frameworks

Answer: B

NEW QUESTION 846

- (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 848

- (Exam Topic 2)

Which of the following should be a risk practitioner's MOST important consideration when developing IT risk scenarios?

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

Answer: C

NEW QUESTION 853

- (Exam Topic 2)

Which of the following BEST indicates that an organizations risk management program is effective?

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

Answer: C

NEW QUESTION 854

- (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 risk

Answer: A

NEW QUESTION 857

- (Exam Topic 2)

Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

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

Answer: B

NEW QUESTION 862

- (Exam Topic 2)

The risk associated with inadvertent disclosure of database records from a public cloud service provider (CSP) would MOST effectively be reduced by:

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

Answer: A

NEW QUESTION 864

- (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 868

- (Exam Topic 2)

Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

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

Answer: D

NEW QUESTION 873

- (Exam Topic 2)

An organization has engaged a third party to provide an Internet gateway encryption service that protects sensitive data uploaded to a cloud service. This is an example of risk:

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

Answer: A

NEW QUESTION 877

- (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 881

- (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 882

- (Exam Topic 2)

Which of the following should be initiated when a high number of noncompliant conditions are observed during review of a control procedure?

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

Answer: D

NEW QUESTION 887

- (Exam Topic 2)

A software developer has administrative access to a production application. Which of the following should be of GREATEST concern to a risk practitioner?

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

Answer: D

NEW QUESTION 891

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 893

- (Exam Topic 2)

Which of the following will BEST help an organization evaluate the control environment of several third-party vendors?

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

Answer: B

NEW QUESTION 897

- (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 901

- (Exam Topic 2)

Which type of cloud computing deployment provides the consumer the GREATEST degree of control over the environment?

- A. Community cloud
- B. Private cloud
- C. Hybrid cloud
- D. Public cloud

Answer: B

NEW QUESTION 904

- (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 908

- (Exam Topic 2)

The MOST important reason to monitor key risk indicators (KRIs) is to help management:

- A. identify 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 913

- (Exam Topic 2)

Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?

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

Answer: A

NEW QUESTION 914

- (Exam Topic 2)

An organization is increasingly concerned about loss of sensitive data and asks the risk practitioner to assess the current risk level. Which of the following should the risk practitioner do FIRST?

- A. Identify staff members who have access to the organization's sensitive data.
- B. Identify locations where the organization's sensitive data is stored.
- C. Identify risk scenarios and owners associated with possible data loss vectors.
- D. Identify existing data loss controls and their levels of effectiveness.

Answer: D

NEW QUESTION 915

- (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 918

- (Exam Topic 2)

Prior to selecting key performance indicators (KPIs), it is MOST important to ensure:

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

Answer: C

NEW QUESTION 922

- (Exam Topic 2)

Which of the following would be MOST relevant to stakeholders regarding ineffective control implementation?

- A. Threat to IT
- B. Number of control failures
- C. Impact on business
- D. Risk ownership

Answer: C

NEW QUESTION 927

- (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 930

- (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 935

- (Exam Topic 2)

Which of the following is the BEST way to support communication of emerging risk?

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

Answer: D

NEW QUESTION 937

- (Exam Topic 2)

Which of the following is the GREATEST concern associated with the transmission of healthcare data across the internet?

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

Answer: A

NEW QUESTION 939

- (Exam Topic 1)

Which of the following would BEST help an enterprise prioritize risk scenarios?

- A. Industry best practices
- B. Placement on the risk map
- C. Degree of variances in the risk
- D. Cost of risk mitigation

Answer: B

NEW QUESTION 941

- (Exam Topic 1)

Which of the following is a PRIMARY benefit of engaging the risk owner during the risk assessment process?

- A. Identification of controls gaps that may lead to noncompliance
- B. Prioritization of risk action plans across departments
- C. Early detection of emerging threats
- D. Accurate measurement of loss impact

Answer: D

NEW QUESTION 945

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 947

- (Exam Topic 1)

A risk practitioner is assisting with the preparation of a report on the organization's disaster recovery (DR) capabilities. Which information would have the MOST impact on the overall recovery profile?

- A. The percentage of systems meeting recovery target times has increased.
- B. The number of systems tested in the last year has increased.
- C. The number of systems requiring a recovery plan has increased.
- D. The percentage of systems with long recovery target times has decreased.

Answer: D

NEW QUESTION 950

- (Exam Topic 1)

Which of the following provides the BEST evidence of the effectiveness of an organization's account provisioning process?

- A. User provisioning
- B. Role-based access controls
- C. Security log monitoring
- D. Entitlement reviews

Answer: D

NEW QUESTION 955

- (Exam Topic 1)

Which of the following should be the risk practitioner's PRIMARY focus when determining whether controls are adequate to mitigate risk?

- A. Sensitivity analysis
- B. Level of residual risk
- C. Cost-benefit analysis
- D. Risk appetite

Answer: C

NEW QUESTION 957

- (Exam Topic 1)

Which of the following is the MOST important consideration when multiple risk practitioners capture risk scenarios in a single risk register?

- A. Aligning risk ownership and control ownership
- B. Developing risk escalation and reporting procedures
- C. Maintaining up-to-date risk treatment plans
- D. Using a consistent method for risk assessment

Answer: D

NEW QUESTION 958

- (Exam Topic 1)

In addition to the risk register, what should a risk practitioner review to develop an understanding of the organization's risk profile?

- A. The control catalog
- B. The asset profile
- C. Business objectives
- D. Key risk indicators (KRIs)

Answer: C

NEW QUESTION 963

- (Exam Topic 1)

Which of the following would be considered a vulnerability?

- A. Delayed removal of employee access
- B. Authorized administrative access to HR files
- C. Corruption of files due to malware
- D. Server downtime due to a denial of service (DoS) attack

Answer: A

NEW QUESTION 967

- (Exam Topic 1)

An organization has identified a risk exposure due to weak technical controls in a newly implemented HR system. The risk practitioner is documenting the risk in the risk register. The risk should be owned by the:

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

Answer: D

NEW QUESTION 972

- (Exam Topic 1)

Which of the following would provide the BEST guidance when selecting an appropriate risk treatment plan?

- A. Risk mitigation budget
- B. Business Impact analysis
- C. Cost-benefit analysis
- D. Return on investment

Answer: C

NEW QUESTION 974

- (Exam Topic 1)

Which of the following would BEST provide early warning of a high-risk condition?

- A. Risk register
- B. Risk assessment
- C. Key risk indicator (KRI)
- D. Key performance indicator (KPI)

Answer: C

NEW QUESTION 978

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CRISC Practice Exam Features:

- * CRISC Questions and Answers Updated Frequently
- * CRISC Practice Questions Verified by Expert Senior Certified Staff
- * CRISC Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CRISC Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CRISC Practice Test Here](#)