

Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control



NEW QUESTION 1

- (Exam Topic 4)

What is the MAIN benefit of using a top-down approach to develop risk scenarios?

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

Answer: C

NEW QUESTION 2

- (Exam Topic 4)

When developing a response plan to address security incidents regarding sensitive data loss, it is MOST important

- A. revalidate current key risk indicators (KRIs).
- B. revise risk management procedures.
- C. review the data classification policy.
- D. revalidate existing risk scenarios.

Answer: C

NEW QUESTION 3

- (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 4

- (Exam Topic 4)

Which of the following is the MOST important consideration for effectively maintaining a risk register?

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

Answer: B

NEW QUESTION 5

- (Exam Topic 4)

A highly regulated enterprise is developing a new risk management plan to specifically address legal and regulatory risk scenarios What should be done FIRST by IT governance to support this effort?

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

Answer: A

NEW QUESTION 6

- (Exam Topic 4)

Which of the following is the PRIMARY accountability for a control owner?

- A. Communicate risk to senior management.
- B. Own the associated risk the control is mitigating.
- C. Ensure the control operates effectively.
- D. Identify and assess control weaknesses.

Answer: C

NEW QUESTION 7

- (Exam Topic 4)

An organization has decided to postpone the assessment and treatment of several risk scenarios because stakeholders are unavailable. As a result of this decision, the risk associated with these new entries has been;

- A. mitigated
- B. deferred

- C. accepted.
- D. transferred

Answer: C

NEW QUESTION 8

- (Exam Topic 4)

An organization's business gap analysis reveals the need for a robust IT risk strategy. Which of the following should be the risk practitioner's PRIMARY consideration when participating in development of the new strategy?

- A. Scale of technology
- B. Risk indicators
- C. Risk culture
- D. Proposed risk budget

Answer: C

NEW QUESTION 9

- (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 10

- (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 10

- (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 14

- (Exam Topic 4)

Using key risk indicators (KRIs) to illustrate changes in the risk profile PRIMARILY helps to:

- A. communicate risk trends to stakeholders.
- B. assign ownership of emerging risk scenarios.
- C. highlight noncompliance with the risk policy
- D. identify threats to emerging technologies.

Answer: A

NEW QUESTION 19

- (Exam Topic 4)

The MOST important measure of the effectiveness of risk management in project implementation is the percentage of projects:

- A. introduced into production without high-risk issues.
- B. having the risk register updated regularly.
- C. having key risk indicators (KRIs) established to measure risk.
- D. having an action plan to remediate overdue issues.

Answer: A

NEW QUESTION 20

- (Exam Topic 4)

Which of the following key performance indicators (KPIs) would BEST measure the risk of a service outage when using a Software as a Service (SaaS) vendors

- A. Frequency of business continuity plan (BCP) testing
- B. Frequency and number of new software releases
- C. Frequency and duration of unplanned downtime
- D. Number of IT support staff available after business hours

Answer: C

NEW QUESTION 24

- (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 25

- (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 26

- (Exam Topic 4)

A risk practitioner notices a risk scenario associated with data loss at the organization's cloud provider is assigned to the provider. Who should the risk scenario be reassigned to?

- A. Senior management
- B. Chief risk officer (CRO)
- C. Vendor manager
- D. Data owner

Answer: D

NEW QUESTION 28

- (Exam Topic 4)

Which component of a software inventory BEST enables the identification and mitigation of known vulnerabilities?

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

Answer: A

NEW QUESTION 33

- (Exam Topic 4)

Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?

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

Answer: B

NEW QUESTION 37

- (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 41

- (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 44

- (Exam Topic 4)

If preventive controls cannot be implemented due to technology limitations, which of the following should be done FIRST to reduce risk?

- A. Evaluate alternative controls.
- B. Redefine the business process to reduce the risk.
- C. Develop a plan to upgrade technology.
- D. Define a process for monitoring risk.

Answer: A

NEW QUESTION 45

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 46

- (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 50

- (Exam Topic 4)

Which of the following is MOST important to determine when assessing the potential risk exposure of a loss event involving personal data?

- A. The cost associated with incident response activities
- B. The maximum levels of applicable regulatory fines
- C. The length of time between identification and containment of the incident
- D. The composition and number of records in the information asset

Answer: C

NEW QUESTION 55

- (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 59

- (Exam Topic 4)

Which of the following is the BEST approach for an organization in a heavily regulated industry to comprehensively test application functionality?

- A. Use production data in a non-production environment
- B. Use masked data in a non-production environment
- C. Use test data in a production environment
- D. Use anonymized data in a non-production environment

Answer:

D

NEW QUESTION 64

- (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 67

- (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 69

- (Exam Topic 3)

Which of The following should be of GREATEST concern for an organization considering the adoption of a bring your own device (BYOD) initiative?

- A. Device corruption
- B. Data loss
- C. Malicious users
- D. User support

Answer: B

NEW QUESTION 71

- (Exam Topic 4)

A recent big data project has resulted in the creation of an application used to support important investment decisions. Which of the following should be of GREATEST concern to the risk practitioner?

- A. Data quality
- B. Maintenance costs
- C. Data redundancy
- D. System integration

Answer: A

NEW QUESTION 74

- (Exam Topic 4)

An organization has allowed several employees to retire early in order to avoid layoffs Many of these employees have been subject matter experts for critical assets Which type of risk is MOST likely to materialize?

- A. Confidentiality breach
- B. Institutional knowledge loss
- C. Intellectual property loss
- D. Unauthorized access

Answer: B

NEW QUESTION 75

- (Exam Topic 4)

Which of the following BEST enables risk-based decision making in support of a business continuity plan (BCP)?

- A. Impact analysis
- B. Control analysis
- C. Root cause analysis
- D. Threat analysis

Answer: A

NEW QUESTION 79

- (Exam Topic 4)

Which of the following resources is MOST helpful to a risk practitioner when updating the likelihood rating in the risk register?

- A. Risk control assessment
- B. Audit reports with risk ratings

- C. Penetration test results
- D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 84

- (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 85

- (Exam Topic 3)

The BEST way to improve a risk register is to ensure the register:

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

Answer: A

NEW QUESTION 86

- (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 90

- (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 95

- (Exam Topic 3)

A financial institution has identified high risk of fraud in several business applications. Which of the following controls will BEST help reduce the risk of fraudulent internal transactions?

- A. Periodic user privileges review
- B. Log monitoring
- C. Periodic internal audits
- D. Segregation of duties

Answer: A

NEW QUESTION 98

- (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 101

- (Exam Topic 3)

The PRIMARY benefit associated with key risk indicators (KRIs) is that they:

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

Answer: D

NEW QUESTION 105

- (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 106

- (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 109

- (Exam Topic 3)

Which of the following is the MOST appropriate key risk indicator (KRI) for backup media that is recycled monthly?

- A. Time required for backup restoration testing
- B. Change in size of data backed up
- C. Successful completion of backup operations
- D. Percentage of failed restore tests

Answer: D

NEW QUESTION 110

- (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 113

- (Exam Topic 3)

When developing a new risk register, a risk practitioner should focus on which of the following risk management activities?

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

Answer: C

NEW QUESTION 114

- (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 119

- (Exam Topic 3)

Which of the following is the MOST important responsibility of a risk owner?

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

Answer: C

NEW QUESTION 122

- (Exam Topic 3)

Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

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

Answer: B

NEW QUESTION 127

- (Exam Topic 3)

While evaluating control costs, management discovers that the annual cost exceeds the annual loss expectancy (ALE) of the risk. This indicates the:

- A. control is ineffective and should be strengthened
- B. risk is inefficiently controlled.
- C. risk is efficiently controlled.
- D. control is weak and should be removed.

Answer: B

NEW QUESTION 128

- (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 133

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 136

- (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 139

- (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 142

- (Exam Topic 3)

Which of the following should be the PRIMARY goal of developing information security metrics?

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

Answer: B

NEW QUESTION 143

- (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 145

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 148

- (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 151

- (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 155

- (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 156

- (Exam Topic 3)

Which of the following would BEST help an enterprise define and communicate its risk appetite?

- A. Gap analysis

- B. Risk assessment
- C. Heat map
- D. Risk register

Answer: C

NEW QUESTION 160

- (Exam Topic 3)

Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information to a supplier?

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

Answer: B

NEW QUESTION 164

- (Exam Topic 3)

Which of the following criteria associated with key risk indicators (KRIs) BEST enables effective risk monitoring?

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

Answer: C

NEW QUESTION 167

- (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 168

- (Exam Topic 3)

Which of the following provides the MOST useful information when determining if a specific control should be implemented?

- A. Business impact analysis (BIA)
- B. Cost-benefit analysis
- C. Attribute analysis
- D. Root cause analysis

Answer: B

NEW QUESTION 172

- (Exam Topic 3)

A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

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

Answer: D

NEW QUESTION 173

- (Exam Topic 3)

The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

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

Answer: C

NEW QUESTION 177

- (Exam Topic 3)

Which of the following provides the MOST useful information to determine risk exposure following control implementations?

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

Answer: C

NEW QUESTION 182

- (Exam Topic 3)

An organization is preparing to transfer a large number of customer service representatives to the sales department. Of the following, who is responsible for mitigating the risk associated with residual system access?

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

Answer: D

NEW QUESTION 187

- (Exam Topic 3)

An organization is conducting a review of emerging risk. Which of the following is the BEST input for this exercise?

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

Answer: B

NEW QUESTION 192

- (Exam Topic 3)

Which of the following is the MOST important consideration for protecting data assets in a Business application system?

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

Answer: A

NEW QUESTION 197

- (Exam Topic 3)

Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

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

Answer: B

NEW QUESTION 198

- (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 199

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 202

- (Exam Topic 3)

What are the MOST essential attributes of an effective Key control indicator (KCI)?

- A. Flexibility and adaptability
- B. Measurability and consistency
- C. Robustness and resilience
- D. Optimal cost and benefit

Answer: B

NEW QUESTION 206

- (Exam Topic 3)

The PRIMARY advantage of involving end users in continuity planning is that they:

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

Answer: B

NEW QUESTION 211

- (Exam Topic 3)

In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

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

Answer: B

NEW QUESTION 215

- (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 220

- (Exam Topic 3)

When reporting on the performance of an organization's control environment including which of the following would BEST inform stakeholders risk decision-making?

- A. The audit plan for the upcoming period
- B. Spend to date on mitigating control implementation
- C. A report of deficiencies noted during controls testing
- D. A status report of control deployment

Answer: C

NEW QUESTION 223

- (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 228

- (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 232

- (Exam Topic 3)

Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

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

Answer: B

NEW QUESTION 237

- (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 240

- (Exam Topic 3)

Which of the following would BEST indicate to senior management that IT processes are improving?

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

Answer: B

NEW QUESTION 244

- (Exam Topic 3)

Which of the following methods is an example of risk mitigation?

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

Answer: C

NEW QUESTION 249

- (Exam Topic 3)

The PRIMARY benefit of using a maturity model is that it helps to evaluate the:

- A. capability to implement new processes
- B. evolution of process improvements
- C. degree of compliance with policies and procedures
- D. control requirements.

Answer: B

NEW QUESTION 252

- (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 254

- (Exam Topic 3)

Which of the following is the BEST source for identifying key control indicators (KCIs)?

- A. Privileged user activity monitoring controls
- B. Controls mapped to organizational risk scenarios
- C. Recent audit findings of control weaknesses

D. A list of critical security processes

Answer: B

NEW QUESTION 255

- (Exam Topic 3)

An organization learns of a new ransomware attack affecting organizations worldwide. Which of the following should be done FIRST to reduce the likelihood of infection from the attack?

- A. Identify systems that are vulnerable to being exploited by the attack.
- B. Confirm with the antivirus solution vendor whether the next update will detect the attack.
- C. Verify the data backup process and confirm which backups are the most recent ones available.
- D. Obtain approval for funding to purchase a cyber insurance plan.

Answer: A

NEW QUESTION 258

- (Exam Topic 3)

Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

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

Answer: B

NEW QUESTION 260

- (Exam Topic 3)

Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

- A. Percentage of unpatched IT assets
- B. Percentage of IT assets without ownership
- C. The number of IT assets securely disposed during the past year
- D. The number of IT assets procured during the previous month

Answer: B

NEW QUESTION 261

- (Exam Topic 4)

Recovery the objectives (RTOs) should be based on

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

Answer: C

NEW QUESTION 266

- (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 268

- (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 271

- (Exam Topic 4)

Reviewing which of the following BEST helps an organization gain insight into its overall risk profile"

- A. Risk register
- B. Risk appetite
- C. Threat landscape
- D. Risk metrics

Answer: B

NEW QUESTION 276

- (Exam Topic 4)

Which of the following BEST enables a risk practitioner to understand management's approach to organizational risk?

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

Answer: B

NEW QUESTION 278

- (Exam Topic 4)

An organization has agreed to a 99% availability for its online services and will not accept availability that falls below 98.5%. This is an example of:

- A. risk mitigation.
- B. risk evaluation.
- C. risk appetite.
- D. risk tolerance.

Answer: C

NEW QUESTION 280

- (Exam Topic 4)

Which of the following provides the MOST useful information to assess the magnitude of identified deficiencies in the IT control environment?

- A. Peer benchmarks
- B. Internal audit reports
- C. Business impact analysis (BIA) results
- D. Threat analysis results

Answer: D

NEW QUESTION 281

- (Exam Topic 4)

Which of the following has the GREATEST influence on an organization's risk appetite?

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

Answer: D

NEW QUESTION 282

- (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 284

- (Exam Topic 4)

Which of the following is MOST important for maintaining the effectiveness of an IT risk register?

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

Answer: D

NEW QUESTION 289

- (Exam Topic 4)

Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

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

Answer: B

NEW QUESTION 291

- (Exam Topic 4)

Which of the following provides the MOST comprehensive information when developing a risk profile for a system?

- A. Results of a business impact analysis (BIA)
- B. Risk assessment results
- C. A mapping of resources to business processes
- D. Key performance indicators (KPIs)

Answer: B

NEW QUESTION 292

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 293

- (Exam Topic 4)

When implementing an IT risk management program, which of the following is the BEST time to evaluate current control effectiveness?

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

Answer: B

NEW QUESTION 296

- (Exam Topic 4)

Which of the following contributes MOST to the effective implementation of risk responses?

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

Answer: A

NEW QUESTION 300

- (Exam Topic 4)

When preparing a risk status report for periodic review by senior management, it is MOST important to ensure the report includes

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

Answer: A

NEW QUESTION 304

- (Exam Topic 4)

Which of the following would MOST likely require a risk practitioner to update the risk register?

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

Answer: C

NEW QUESTION 308

- (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 310

- (Exam Topic 4)

An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

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

Answer: D

NEW QUESTION 312

- (Exam Topic 4)

Who is MOST important to include in the assessment of existing IT risk scenarios?

- A. Technology subject matter experts
- B. Business process owners
- C. Business users of IT systems
- D. Risk management consultants

Answer: C

NEW QUESTION 315

- (Exam Topic 4)

An organization wants to grant remote access to a system containing sensitive data to an overseas third party. Which of the following should be of GREATEST concern to management?

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

Answer: C

NEW QUESTION 316

- (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 319

- (Exam Topic 4)

Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

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

Answer: A

NEW QUESTION 320

- (Exam Topic 4)

Which of the following would be a risk practitioner's BEST course of action when a project team has accepted a risk outside the established risk appetite?

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

D. Document the risk decision in the project risk register.

Answer: B

NEW QUESTION 323

- (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 326

- (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 329

- (Exam Topic 4)

Which of the following is the BEST recommendation to address recent IT risk trends that indicate social engineering attempts are increasing in the organization?

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

Answer: A

NEW QUESTION 330

- (Exam Topic 4)

Which of the following would be the result of a significant increase in the motivation of a malicious threat actor?

- A. Increase in mitigating control costs
- B. Increase in risk event impact
- C. Increase in risk event likelihood
- D. Increase in cybersecurity premium

Answer: C

NEW QUESTION 333

- (Exam Topic 4)

Which of the following is the PRIMARY reason to engage business unit managers in risk management processes'?

- A. Improved alignment with technical risk
- B. Better-informed business decisions
- C. Enhanced understanding of enterprise architecture (EA)
- D. Improved business operations efficiency

Answer: C

NEW QUESTION 335

- (Exam Topic 4)

Which of the following BEST facilitates the identification of appropriate key performance indicators (KPIs) for a risk management program?

- A. Reviewing control objectives
- B. Aligning with industry best practices
- C. Consulting risk owners
- D. Evaluating KPIs in accordance with risk appetite

Answer: C

NEW QUESTION 340

- (Exam Topic 4)

Which of the following is the BEST method to mitigate the risk of an unauthorized employee viewing confidential data in a database"

- A. Implement role-based access control
- B. Implement a data masking process
- C. Include sanctions in nondisclosure agreements (NDAs)
- D. Install a data loss prevention (DLP) tool

Answer: A

NEW QUESTION 342

- (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 343

- (Exam Topic 4)

An organization plans to implement a new Software as a Service (SaaS) speech-to-text solution Which of the following is MOST important to mitigate risk associated with data privacy?

- A. Secure encryption protocols are utilized.
- B. Multi-factor authentication is set up for users.
- C. The solution architecture is approved by IT.
- D. A risk transfer clause is included in the contract

Answer: A

NEW QUESTION 346

- (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 348

- (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 349

- (Exam Topic 4)

An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?

- A. Acquisition
- B. Implementation
- C. Initiation
- D. Operation and maintenance

Answer: C

NEW QUESTION 350

- (Exam Topic 4)

Which of the following is MOST important to promoting a risk-aware culture?

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

Answer: D

NEW QUESTION 353

- (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 355

- (Exam Topic 4)

Which of the following BEST helps to identify significant events that could impact an organization?

- A. Control analysis
- B. Vulnerability analysis
- C. Scenario analysis
- D. Heat map analysis

Answer: C

NEW QUESTION 358

- (Exam Topic 4)

Which of the following is MOST helpful in providing an overview of an organization's risk management program?

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

Answer: C

NEW QUESTION 360

- (Exam Topic 4)

Which of the following is the BEST approach for selecting controls to minimize risk?

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

Answer: C

NEW QUESTION 362

- (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 366

- (Exam Topic 4)

Which of the following would be the BEST way for a risk practitioner to validate the effectiveness of a patching program?

- A. Conduct penetration testing.
- B. Interview IT operations personnel.
- C. Conduct vulnerability scans.
- D. Review change control board documentation.

Answer: C

NEW QUESTION 368

- (Exam Topic 4)

Effective risk communication BEST benefits an organization by:

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

Answer:

A

NEW QUESTION 372

- (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 373

- (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 376

- (Exam Topic 4)

Who is the BEST person to the employee personal data?

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

Answer: A

NEW QUESTION 379

- (Exam Topic 4)

Which of the following is the MOST useful information for a risk practitioner when planning response activities after risk identification?

- A. Risk register
- B. Risk appetite
- C. Risk priorities
- D. Risk heat maps

Answer: B

NEW QUESTION 384

- (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 386

- (Exam Topic 4)

When evaluating a number of potential controls for treating risk, it is MOST important to consider:

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

Answer: C

NEW QUESTION 387

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 388

- (Exam Topic 4)

Which of the following is MOST important to determine as a result of a risk assessment?

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

Answer: D

NEW QUESTION 392

- (Exam Topic 4)

Which of the following is the GREATEST benefit of a three lines of defense structure?

- A. An effective risk culture that empowers employees to report risk
- B. Effective segregation of duties to prevent internal fraud
- C. Clear accountability for risk management processes
- D. Improved effectiveness and efficiency of business operations

Answer: C

NEW QUESTION 394

- (Exam Topic 4)

During a risk assessment, a risk practitioner learns that an IT risk factor is adequately mitigated by compensating controls in an associated business process. Which of the following would enable the MOST effective management of the residual risk?

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

Answer: A

NEW QUESTION 399

- (Exam Topic 4)

The BEST key performance indicator (KPI) to measure the effectiveness of the security patching process is the percentage of patches installed:

- A. by the security administration team.
- B. successfully within the expected time frame.
- C. successfully during the first attempt.
- D. without causing an unplanned system outage.

Answer: B

NEW QUESTION 400

- (Exam Topic 4)

it was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern?

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

Answer: C

NEW QUESTION 404

- (Exam Topic 4)

Which of the following is a risk practitioner's BEST course of action after identifying risk scenarios related to noncompliance with new industry regulations?

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

Answer: D

NEW QUESTION 405

- (Exam Topic 3)

What information is MOST helpful to asset owners when classifying organizational assets for risk assessment?

- A. Potential loss to the business due to non-performance of the asset
- B. Known emerging environmental threats

- C. Known vulnerabilities published by the asset developer
- D. Cost of replacing the asset with a new asset providing similar services

Answer: A

NEW QUESTION 408

- (Exam Topic 3)

A risk practitioner has just learned about new malware that has severely impacted industry peers worldwide data loss?

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

Answer: B

NEW QUESTION 411

- (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 415

- (Exam Topic 3)

Which of the following would be MOST helpful to an information security management team when allocating resources to mitigate exposures?

- A. Relevant risk case studies
- B. Internal audit findings
- C. Risk assessment results
- D. Penetration testing results

Answer: C

NEW QUESTION 419

- (Exam Topic 3)

When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

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

Answer: B

NEW QUESTION 422

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 424

- (Exam Topic 3)

An information system for a key business operation is being moved from an in-house application to a Software as a Service (SaaS) vendor. Which of the following will have the GREATEST impact on the ability to monitor risk?

- A. Reduced ability to evaluate key risk indicators (KRIs)
- B. Reduced access to internal audit reports
- C. Dependency on the vendor's key performance indicators (KPIs)
- D. Dependency on service level agreements (SLAs)

Answer: A

NEW QUESTION 425

- (Exam Topic 3)

Which element of an organization's risk register is MOST important to update following the commissioning of a new financial reporting system?

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

Answer: C

NEW QUESTION 427

- (Exam Topic 3)

Which of the following is MOST important to communicate to senior management during the initial implementation of a risk management program?

- A. Regulatory compliance
- B. Risk ownership
- C. Best practices
- D. Desired risk level

Answer: D

NEW QUESTION 430

- (Exam Topic 3)

Which of the following BEST indicates that additional or improved controls are needed in the environment?

- A. Management has decreased organisational risk appetite
- B. The risk register and portfolio do not include all risk scenarios
- C. Merging risk scenarios have been identified
- D. Risk events and losses exceed risk tolerance

Answer: D

NEW QUESTION 434

- (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 439

- (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 441

- (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 442

- (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 443

- (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 445

- (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 447

- (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 framework
- D. A roadmap of IT strategic planning

Answer: B

NEW QUESTION 450

- (Exam Topic 3)

Which of the following should be done FIRST when developing a data protection management plan?

- A. Perform a cost-benefit analysis.
- B. Identify critical data.
- C. Establish a data inventory.
- D. Conduct a risk analysis.

Answer: B

NEW QUESTION 453

- (Exam Topic 3)

An employee lost a personal mobile device that may contain sensitive corporate information. What should be the risk practitioner's recommendation?

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

Answer: C

NEW QUESTION 457

- (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 461

- (Exam Topic 3)

An organization automatically approves exceptions to security policies on a recurring basis. This practice is MOST likely the result of:

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

Answer: D

NEW QUESTION 464

- (Exam Topic 3)

The BEST indication that risk management is effective is when risk has been reduced to meet:

- A. risk levels.
- B. risk budgets.
- C. risk appetite.
- D. risk capacity.

Answer: C

NEW QUESTION 466

- (Exam Topic 3)

Which of the following BEST indicates the effectiveness of anti-malware software?

- A. Number of staff hours lost due to malware attacks
- B. Number of downtime hours in business critical servers
- C. Number of patches made to anti-malware software
- D. Number of successful attacks by malicious software

Answer: D

NEW QUESTION 468

- (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 470

- (Exam Topic 3)

Which of the following should a risk practitioner recommend FIRST when an increasing trend of risk events and subsequent losses has been identified?

- A. Conduct root cause analyses for risk events.
- B. Educate personnel on risk mitigation strategies.
- C. Integrate the risk event and incident management processes.
- D. Implement controls to prevent future risk events.

Answer: C

NEW QUESTION 471

- (Exam Topic 3)

Which of the following is the BEST way to assess the effectiveness of an access management process?

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

Answer: B

NEW QUESTION 476

- (Exam Topic 3)

The MAIN purpose of reviewing a control after implementation is to validate that the control:

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

Answer: A

NEW QUESTION 480

- (Exam Topic 3)

A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

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

Answer: A

NEW QUESTION 483

- (Exam Topic 3)

Which of the following is a drawback in the use of quantitative risk analysis?

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

Answer: B

NEW QUESTION 488

- (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 491

- (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 492

- (Exam Topic 3)

Which of the following should be done FIRST when information is no longer required to support business objectives?

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

Answer: C

NEW QUESTION 493

- (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 495

- (Exam Topic 3)

In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

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

Answer: B

NEW QUESTION 497

- (Exam Topic 3)

Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?

- A. Relevance to the business process
- B. Regulatory compliance requirements

- C. Cost-benefit analysis
- D. Comparison against best practice

Answer: B

NEW QUESTION 500

- (Exam Topic 3)

Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

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

Answer: A

NEW QUESTION 501

- (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-virjns software updates

Answer: A

NEW QUESTION 502

- (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 504

- (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 509

- (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 513

- (Exam Topic 2)

An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

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

Answer: A

NEW QUESTION 516

- (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 517

- (Exam Topic 2)

When reviewing a risk response strategy, senior management's PRIMARY focus should be placed on the:

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

Answer: D

NEW QUESTION 522

- (Exam Topic 2)

Mapping open risk issues to an enterprise risk heat map BEST facilitates:

- A. risk response.
- B. control monitoring.
- C. risk identification.
- D. risk ownership.

Answer: A

NEW QUESTION 526

- (Exam Topic 2)

When collecting information to identify IT-related risk, a risk practitioner should FIRST focus on IT:

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

Answer: B

NEW QUESTION 531

- (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 535

- (Exam Topic 2)

IT disaster recovery point objectives (RPOs) should be based on the:

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

Answer: C

NEW QUESTION 539

- (Exam Topic 2)

An organization's risk practitioner learns a new third-party system on the corporate network has introduced vulnerabilities that could compromise corporate IT systems. What should the risk practitioner do FIRST?

- A. Confirm the vulnerabilities with the third party
- B. Identify procedures to mitigate the vulnerabilities.
- C. Notify information security management.
- D. Request IT to remove the system from the network.

Answer: B

NEW QUESTION 542

- (Exam Topic 2)

Which of The following is the MOST relevant information to include in a risk management strategy?

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

Answer: D

NEW QUESTION 547

- (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 552

- (Exam Topic 2)

A risk practitioner shares the results of a vulnerability assessment for a critical business application with the business manager. Which of the following is the NEXT step?

- A. Develop a risk action plan to address the findings.
- B. Evaluate the impact of the vulnerabilities to the business application.
- C. Escalate the findings to senior management and internal audit.
- D. Conduct a penetration test to validate the vulnerabilities from the findings.

Answer: B

NEW QUESTION 557

- (Exam Topic 2)

Which of the following is a detective control?

- A. Limit check
- B. Periodic access review
- C. Access control software
- D. Rerun procedures

Answer: B

NEW QUESTION 560

- (Exam Topic 2)

An organization has granted a vendor access to its data in order to analyze customer behavior. Which of the following would be the MOST effective control to mitigate the risk of customer data leakage?

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

Answer: D

NEW QUESTION 562

- (Exam Topic 2)

Which of the following provides the MOST helpful information in identifying risk in an organization?

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

Answer: C

NEW QUESTION 567

- (Exam Topic 2)

Which of the following is a KEY outcome of risk ownership?

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

Answer: A

NEW QUESTION 571

- (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 574

- (Exam Topic 2)

Which of the following is the BEST way to detect zero-day malware on an end user's workstation?

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

Answer: C

NEW QUESTION 578

- (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 583

- (Exam Topic 2)

Which of the following BEST enables a proactive approach to minimizing the potential impact of unauthorized data disclosure?

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

Answer: C

NEW QUESTION 586

- (Exam Topic 2)

Which of the following BEST promotes commitment to controls?

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

Answer: A

NEW QUESTION 589

- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to ensure once a risk action plan has been completed?

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

Answer: B

NEW QUESTION 594

- (Exam Topic 2)

Which of the following BEST enables the risk profile to serve as an effective resource to support business objectives?

- A. Engaging external risk professionals to periodically review the risk
- B. Prioritizing global standards over local requirements in the risk profile

- C. Updating the risk profile with risk assessment results
- D. Assigning quantitative values to qualitative metrics in the risk register

Answer: C

NEW QUESTION 597

- (Exam Topic 2)

Which of the following would provide the MOST objective assessment of the effectiveness of an organization's security controls?

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

Answer: D

NEW QUESTION 598

- (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 603

- (Exam Topic 2)

When testing the security of an IT system, it is MOST important to ensure that;

- A. tests are conducted after business hours.
- B. operators are unaware of the test.
- C. external experts execute the test.
- D. agreement is obtained from stakeholders.

Answer: D

NEW QUESTION 608

- (Exam Topic 2)

A department has been granted an exception to bypass the existing approval process for purchase orders. The risk practitioner should verify the exception has been approved by which of the following?

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

Answer: B

NEW QUESTION 613

- (Exam Topic 2)

As part of an overall IT risk management plan, an IT risk register BEST helps management:

- A. align IT processes with business objectives.
- B. communicate the enterprise risk management policy.
- C. stay current with existing control status.
- D. understand the organizational risk profile.

Answer: D

NEW QUESTION 615

- (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 617

- (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 618

- (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 621

- (Exam Topic 2)

An IT operations team implements disaster recovery controls based on decisions from application owners regarding the level of resiliency needed. Who is the risk owner in this scenario?

- A. Business resilience manager
- B. Disaster recovery team lead
- C. Application owner
- D. IT operations manager

Answer: C

NEW QUESTION 624

- (Exam Topic 2)

Which of the following is the MAIN benefit of involving stakeholders in the selection of key risk indicators (KRIs)?

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

Answer: B

NEW QUESTION 629

- (Exam Topic 2)

Which of the following should be the PRIMARY objective of a risk awareness training program?

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

Answer: A

NEW QUESTION 630

- (Exam Topic 2)

Which of the following should an organization perform to forecast the effects of a disaster?

- A. Develop a business impact analysis (BIA).
- B. Define recovery time objectives (RTO).
- C. Analyze capability maturity model gaps.
- D. Simulate a disaster recovery.

Answer: A

NEW QUESTION 635

- (Exam Topic 2)

Which of the following is the FIRST step when developing a business case to drive the adoption of a risk remediation project by senior management?

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

Answer: A

NEW QUESTION 638

- (Exam Topic 2)

A risk practitioner recently discovered that sensitive data 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. Implement equivalent security in the test environment.
- C. Prevent the use of production data for test purposes
- D. Mask data before being transferred to the test environment.

Answer: B

NEW QUESTION 643

- (Exam Topic 2)

Which of the following is MOST helpful to review when identifying risk scenarios associated with the adoption of Internet of Things (IoT) technology in an organization?

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

Answer: B

NEW QUESTION 646

- (Exam Topic 2)

Which of the following is the MOST effective way to mitigate identified risk scenarios?

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

Answer: A

NEW QUESTION 648

- (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 651

- (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 654

- (Exam Topic 2)

Which of the following is the MOST important consideration when determining whether to accept residual risk after security controls have been implemented on a critical system?

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

Answer: A

NEW QUESTION 656

- (Exam Topic 2)

Which of the following should be the MAIN consideration when validating an organization's risk appetite?

- A. Comparison against regulations
- B. Maturity of the risk culture
- C. Capacity to withstand loss
- D. Cost of risk mitigation options

Answer: B

NEW QUESTION 661

- (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 665

- (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 669

- (Exam Topic 2)

Which of The following will BEST communicate the importance of risk mitigation initiatives to senior management?

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

Answer: A

NEW QUESTION 672

- (Exam Topic 2)

Which of the following is the PRIMARY reason for an organization to ensure the risk register is updated regularly?

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

Answer: D

NEW QUESTION 674

- (Exam Topic 2)

To minimize risk in a software development project, when is the BEST time to conduct a risk analysis?

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

Answer: A

NEW QUESTION 676

- (Exam Topic 2)

Which of the following is the BEST course of action when risk is found to be above the acceptable risk appetite?

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

Answer: D

NEW QUESTION 678

- (Exam Topic 2)

Which of The following would offer the MOST insight with regard to an organization's risk culture?

- A. Risk management procedures
- B. Senior management interviews

- C. Benchmark analyses
- D. Risk management framework

Answer: B

NEW QUESTION 683

- (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 686

- (Exam Topic 2)

A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

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

Answer: C

NEW QUESTION 688

- (Exam Topic 2)

A risk practitioner notices a trend of noncompliance with an IT-related control. Which of the following would BEST assist in making a recommendation to management?

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

Answer: A

NEW QUESTION 690

- (Exam Topic 2)

Which of the following is the PRIMARY objective for automating controls?

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

Answer: A

NEW QUESTION 692

- (Exam Topic 2)

An organization is considering adopting artificial intelligence (AI). Which of the following is the risk practitioner's MOST important course of action?

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

Answer: C

NEW QUESTION 695

- (Exam Topic 2)

Which of the following would BEST enable a risk practitioner to embed risk management within the organization?

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

Answer: D

NEW QUESTION 696

- (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 697

- (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 702

- (Exam Topic 2)

The risk appetite for an organization could be derived from which of the following?

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

Answer: A

NEW QUESTION 707

- (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 710

- (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 711

- (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 715

- (Exam Topic 2)

Which of the following is MOST effective in continuous risk management process improvement?

- A. Periodic assessments
- B. Change management
- C. Awareness training
- D. Policy updates

Answer: A

NEW QUESTION 719

- (Exam Topic 2)

An organization's financial analysis department uses an in-house forecasting application for business projections. Who is responsible for defining access roles to protect the sensitive data within this application?

- A. IT risk manager
- B. IT system owner
- C. Information security manager
- D. Business owner

Answer: D

NEW QUESTION 722

- (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 727

- (Exam Topic 2)

Who should be responsible for implementing and maintaining security controls?

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

Answer: C

NEW QUESTION 731

- (Exam Topic 2)

Read" rights to application files in a controlled server environment should be approved by the:

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

Answer: A

NEW QUESTION 736

- (Exam Topic 2)

An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

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

Answer: B

NEW QUESTION 740

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 743

- (Exam Topic 2)

What is MOST important for the risk practitioner to understand when creating an initial IT risk register?

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

D. Organizational objectives

Answer: D

NEW QUESTION 745

- (Exam Topic 2)

Which of the following controls would BEST reduce the likelihood of a successful network attack through social engineering?

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

Answer: B

NEW QUESTION 750

- (Exam Topic 2)

A bank wants to send a critical payment order via email to one of its offshore branches. Which of the following is the BEST way to ensure the message reaches the intended recipient without alteration?

- A. Add a digital certificate
- B. Apply multi-factor authentication
- C. Add a hash to the message
- D. Add a secret key

Answer: C

NEW QUESTION 755

- (Exam Topic 2)

A risk owner has accepted a high-impact risk because the control was adversely affecting process efficiency. Before updating the risk register, it is MOST important for the risk practitioner to:

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

Answer: D

NEW QUESTION 758

- (Exam Topic 2)

Which of the following is the MOST important reason to revisit a previously accepted risk?

- A. To update risk ownership
- B. To review the risk acceptance with new stakeholders
- C. To ensure risk levels have not changed
- D. To ensure controls are still operating effectively

Answer: C

NEW QUESTION 762

- (Exam Topic 2)

A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration when establishing a contingency plan and an alternate processing site?

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

Answer: B

NEW QUESTION 766

- (Exam Topic 2)

Which of the following is the MAIN reason for analyzing risk scenarios?

- A. Identifying additional risk scenarios
- B. Updating the heat map
- C. Assessing loss expectancy
- D. Establishing a risk appetite

Answer: C

NEW QUESTION 771

- (Exam Topic 2)

What should a risk practitioner do FIRST when vulnerability assessment results identify a weakness in an application?

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

Answer: C

NEW QUESTION 772

- (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 773

- (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 777

- (Exam Topic 2)

Which of the following would BEST help secure online financial transactions from improper users?

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

Answer: D

NEW QUESTION 782

- (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 786

- (Exam Topic 2)

An organization has raised the risk appetite for technology risk. The MOST likely result would be:

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

Answer: D

NEW QUESTION 790

- (Exam Topic 2)

Which of the following is a risk practitioner's BEST course of action upon learning that a control under internal review may no longer be necessary?

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

Answer: B

NEW QUESTION 795

- (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 797

- (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 801

- (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 802

- (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 804

- (Exam Topic 2)

Which of the following statements BEST describes risk appetite?

- A. The amount of risk an organization is willing to accept
- B. The effective management of risk and internal control environments
- C. Acceptable variation between risk thresholds and business objectives
- D. The acceptable variation relative to the achievement of objectives

Answer: A

NEW QUESTION 805

- (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 806

- (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 810

- (Exam Topic 2)

Which of the following BEST contributes to the implementation of an effective risk response action plan?

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

Answer: C

NEW QUESTION 811

- (Exam Topic 2)

Which of the following should be of GREATEST concern to a risk practitioner when determining the effectiveness of IT controls?

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

Answer: A

NEW QUESTION 813

- (Exam Topic 2)

Of the following, who should be responsible for determining the inherent risk rating of an application?

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

Answer: C

NEW QUESTION 817

- (Exam Topic 2)

Which of the following presents the GREATEST challenge for an IT risk practitioner who wants to report on trends in historical IT risk levels?

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

Answer: A

NEW QUESTION 822

- (Exam Topic 2)

Once a risk owner has decided to implement a control to mitigate risk, it is MOST important to develop:

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

Answer: A

NEW QUESTION 825

- (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 828

- (Exam Topic 2)

Performing a background check on a new employee candidate before hiring is an example of what type of control?

- A. Detective
- B. Compensating
- C. Corrective
- D. Preventive

Answer: C

NEW QUESTION 829

- (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 830

- (Exam Topic 2)

Which of the following is MOST important to review when determining whether a potential IT service provider's control environment is effective?

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

Answer: A

NEW QUESTION 834

- (Exam Topic 2)

The effectiveness of a control has decreased. What is the MOST likely effect on the associated risk?

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

Answer: D

NEW QUESTION 837

- (Exam Topic 2)

Which of the following is MOST helpful to management when determining the resources needed to mitigate a risk?

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

Answer: C

NEW QUESTION 838

- (Exam Topic 2)

A risk practitioner learns that the organization's industry is experiencing a trend of rising security incidents. Which of the following is the BEST course of action?

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

Answer: A

NEW QUESTION 839

- (Exam Topic 2)

A large organization needs to report risk at all levels for a new centralized visualization project to reduce cost and improve performance. Which of the following would MOST effectively represent the overall risk of the project to senior management?

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

Answer: D

NEW QUESTION 840

- (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 844

- (Exam Topic 2)

What should be the PRIMARY objective for a risk practitioner performing a post-implementation review of an IT risk mitigation project?

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

Answer: D

NEW QUESTION 846

- (Exam Topic 1)

Which of the following is the MOST important foundational element of an effective three lines of defense model for an organization?

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

Answer: B

NEW QUESTION 849

- (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 852

- (Exam Topic 1)

Which of the following would be MOST helpful to understand the impact of a new technology system on an organization's current risk profile?

- A. Hire consultants specializing in the new technology.
- B. Review existing risk mitigation controls.
- C. Conduct a gap analysis.
- D. Perform a risk assessment.

Answer: D

NEW QUESTION 857

- (Exam Topic 1)

Which of the following is the BEST metric to demonstrate the effectiveness of an organization's change management process?

- A. Increase in the frequency of changes
- B. Percent of unauthorized changes
- C. Increase in the number of emergency changes
- D. Average time to complete changes

Answer: B

NEW QUESTION 860

- (Exam Topic 1)

Establishing and organizational code of conduct is an example of which type of control?

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

Answer: B

NEW QUESTION 863

- (Exam Topic 1)

A global organization is considering the acquisition of a competitor. Senior management has requested a review of the overall risk profile from the targeted organization. Which of the following components of this review would provide the MOST useful information?

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

Answer: D

NEW QUESTION 868

- (Exam Topic 1)

Which of the following is the BEST way to validate the results of a vulnerability assessment?

- A. Perform a penetration test.
- B. Review security logs.
- C. Conduct a threat analysis.
- D. Perform a root cause analysis.

Answer: A

NEW QUESTION 869

- (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 873

- (Exam Topic 1)

Which of the following elements of a risk register is MOST likely to change as a result of change in management's risk appetite?

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

Answer: A

NEW QUESTION 877

- (Exam Topic 1)

A risk practitioner discovers several key documents detailing the design of a product currently in development have been posted on the Internet. What should be the risk practitioner's FIRST course of action?

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

Answer: A

NEW QUESTION 878

- (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 881

- (Exam Topic 1)

An organization that has been the subject of multiple social engineering attacks is developing a risk awareness program. The PRIMARY goal of this program should be to:

- A. reduce the risk to an acceptable level.
- B. communicate the consequences for violations.
- C. implement industry best practices.
- D. reduce the organization's risk appetite

Answer: B

NEW QUESTION 884

- (Exam Topic 1)

Which of the following is the BEST way to identify changes to the risk landscape?

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

Answer: C

NEW QUESTION 888

- (Exam Topic 1)

Calculation of the recovery time objective (RTO) is necessary to determine the:

- A. time required to restore files.
- B. point of synchronization
- C. priority of restoration.
- D. annual loss expectancy (ALE).

Answer: A

NEW QUESTION 892

- (Exam Topic 1)

Which of the following should be the PRIMARY consideration when assessing the automation of control monitoring?

- A. impact due to failure of control
- B. Frequency of failure of control
- C. Contingency plan for residual risk
- D. Cost-benefit analysis of automation

Answer: D

NEW QUESTION 893

- (Exam Topic 1)

Which of the following should be the HIGHEST priority when developing a risk response?

- A. The risk response addresses the risk with a holistic view.
- B. The risk response is based on a cost-benefit analysis.
- C. The risk response is accounted for in the budget.
- D. The risk response aligns with the organization's risk appetite.

Answer: D

NEW QUESTION 898

- (Exam Topic 1)

Which of the following is the MOST important benefit of key risk indicators (KRIs)?

- A. Assisting in continually optimizing risk governance
- B. Enabling the documentation and analysis of trends
- C. Ensuring compliance with regulatory requirements
- D. Providing an early warning to take proactive actions

Answer: D

NEW QUESTION 902

- (Exam Topic 1)

Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?

- A. Assess the vulnerability management process.
- B. Conduct a control self-assessment.
- C. Conduct a vulnerability assessment.
- D. Reassess the inherent risk of the target.

Answer: A

NEW QUESTION 904

- (Exam Topic 1)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery plan (DRP)?

- A. Number of users that participated in the DRP testing
- B. Number of issues identified during DRP testing
- C. Percentage of applications that met the RTO during DRP testing
- D. Percentage of issues resolved as a result of DRP testing

Answer:

B

NEW QUESTION 906

- (Exam Topic 1)

Which of the following would BEST help to ensure that suspicious network activity is identified?

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

Answer: A

NEW QUESTION 907

- (Exam Topic 1)

Which of the following is MOST effective against external threats to an organizations confidential information?

- A. Single sign-on
- B. Data integrity checking
- C. Strong authentication
- D. Intrusion detection system

Answer: C

NEW QUESTION 911

.....

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](#)