

Exam Questions CRISC

Certified in Risk and Information Systems Control

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



NEW QUESTION 1

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

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)

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

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

Answer: A

NEW QUESTION 5

- (Exam Topic 4)

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 6

- (Exam Topic 4)

Which of the following would provide the MOST reliable evidence of the effectiveness of security controls implemented for a web application?

- A. Penetration testing
- B. IT general controls audit
- C. Vulnerability assessment
- D. Fault tree analysis

Answer: A

NEW QUESTION 7

- (Exam Topic 4)

The BEST metric to demonstrate that servers are configured securely is the total number of servers:

- A. exceeding availability thresholds
- B. experiencing hardware failures

- C. exceeding current patching standards.
- D. meeting the baseline for hardening.

Answer: D

NEW QUESTION 8

- (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 9

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 10

- (Exam Topic 4)

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 10

- (Exam Topic 4)

A core data center went offline abruptly for several hours affecting many transactions across multiple locations. Which of the following would provide the MOST useful information to determine mitigating controls?

- A. Forensic analysis
- B. Risk assessment
- C. Root cause analysis
- D. Business impact analysis (BIA)

Answer: A

NEW QUESTION 12

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 13

- (Exam Topic 4)

An organization's control environment is MOST effective when:

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

Answer: A

NEW QUESTION 15

- (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 17

- (Exam Topic 4)

Which of the following is PRIMARILY a risk management responsibility of the first line of defense?

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

Answer: C

NEW QUESTION 20

- (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 24

- (Exam Topic 4)

An organization has decided to implement a new Internet of Things (IoT) solution. Which of the following should be done FIRST when addressing security concerns associated with this new technology?

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

Answer: A

NEW QUESTION 27

- (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 31

- (Exam Topic 4)

A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

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

Answer: B

NEW QUESTION 33

- (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 35

- (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 38

- (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 41

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 45

- (Exam Topic 4)

Which of the following practices would be MOST effective in protecting personally identifiable information (PII) from unauthorized access in a cloud environment?

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

Answer: B

NEW QUESTION 49

- (Exam Topic 4)

Which of the following would be a risk practitioner's GREATEST concern with the use of a vulnerability scanning tool?

- A. Increased time to remediate vulnerabilities
- B. Inaccurate reporting of results
- C. Increased number of vulnerabilities
- D. Network performance degradation

Answer: B

NEW QUESTION 54

- (Exam Topic 4)

An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis. Which of the following is the MOST important control to ensure the privacy of customer information?

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

Answer: C

NEW QUESTION 55

- (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 59

- (Exam Topic 4)

Which of the following is the MOST effective way to help ensure accountability for managing risk?

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

Answer: A

NEW QUESTION 60

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 64

- (Exam Topic 4)

A MAJOR advantage of using key risk indicators (KRIs) is that (hey

- A. identify when risk exceeds defined thresholds
- B. assess risk scenarios that exceed defined thresholds
- C. identify scenarios that exceed defined risk appetite
- D. help with internal control assessments concerning risk appetite

Answer: B

NEW QUESTION 68

- (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 4)

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

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

Answer: C

NEW QUESTION 71

- (Exam Topic 3)

A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

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

Answer: A

NEW QUESTION 75

- (Exam Topic 4)

Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?

- A. Updating the organizational policy for remote access

- B. Creating metrics to track remote connections
- C. Implementing multi-factor authentication
- D. Updating remote desktop software

Answer: A

NEW QUESTION 78

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 79

- (Exam Topic 4)

Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?

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

Answer: D

NEW QUESTION 83

- (Exam Topic 4)

A penetration test reveals several vulnerabilities in a web-facing application. Which of the following should be the FIRST step in selecting a risk response?

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

Answer: C

NEW QUESTION 86

- (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 87

- (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 88

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 90

- (Exam Topic 3)

Which of the following is the MOST effective control to maintain the integrity of system configuration files?

- A. Recording changes to configuration files
- B. Implementing automated vulnerability scanning
- C. Restricting access to configuration documentation
- D. Monitoring against the configuration standard

Answer: D

NEW QUESTION 95

- (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 99

- (Exam Topic 3)

An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course of action?

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

Answer: B

NEW QUESTION 102

- (Exam Topic 3)

During a risk treatment plan review, a risk practitioner finds the approved risk action plan has not been completed. However, there were other risk mitigation actions implemented. Which of the following is the BEST course of action?

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

Answer: A

NEW QUESTION 107

- (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 108

- (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 112

- (Exam Topic 3)

When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

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

Answer: D

NEW QUESTION 113

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 117

- (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 118

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 123

- (Exam Topic 3)

Which of the following should be considered when selecting a risk response?

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

Answer: B

NEW QUESTION 127

- (Exam Topic 3)

The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:

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

Answer: A

NEW QUESTION 128

- (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 132

- (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 134

- (Exam Topic 3)

An organization has detected unauthorized logins to its client database servers. Which of the following should be of GREATEST concern?

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

Answer: C

NEW QUESTION 137

- (Exam Topic 3)

Which of the following would require updates to an organization's IT risk register?

- A. Discovery of an ineffectively designed key IT control
- B. Management review of key risk indicators (KRIs)
- C. Changes to the team responsible for maintaining the register
- D. Completion of the latest internal audit

Answer: A

NEW QUESTION 138

- (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 141

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 142

- (Exam Topic 3)

Which of the following is the MOST important topic to cover in a risk awareness training program for all staff?

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

Answer: C

NEW QUESTION 145

- (Exam Topic 3)

Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

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

Answer: D

NEW QUESTION 150

- (Exam Topic 3)

Which of the following should be an element of the risk appetite of an organization?

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

Answer: B

NEW QUESTION 152

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 157

- (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 158

- (Exam Topic 3)

When of the following is the BEST key control indicator (KCI) to determine the effectiveness of an intrusion prevention system (IPS)?

- A. Percentage of system uptime
- B. Percentage of relevant threats mitigated
- C. Total number of threats identified
- D. Reaction time of the system to threats

Answer: B

NEW QUESTION 162

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 164

- (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 165

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 167

- (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 169

- (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 170

- (Exam Topic 3)

Which of the following is MOST helpful in aligning IT risk with business objectives?

- A. Introducing an approved IT governance framework
- B. Integrating the results of top-down risk scenario analyses
- C. Performing a business impact analysis (BIA)
- D. Implementing a risk classification system

Answer: C

NEW QUESTION 173

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 176

- (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 180

- (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 181

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 183

- (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 184

- (Exam Topic 3)

While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

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

Answer: B

NEW QUESTION 189

- (Exam Topic 3)

When of the following is the MOST significant exposure when an application uses individual user accounts to access the underlying database?

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

Answer: C

NEW QUESTION 190

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 193

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 194

- (Exam Topic 3)

A risk practitioner has been asked to advise management on developing a log collection and correlation strategy. Which of the following should be the MOST important consideration when developing this strategy?

- A. Ensuring time synchronization of log sources.
- B. Ensuring the inclusion of external threat intelligence log sources.
- C. Ensuring the inclusion of all computing resources as log sources.
- D. Ensuring read-write access to all log sources

Answer: A

NEW QUESTION 198

- (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 203

- (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 207

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 209

- (Exam Topic 3)

Which of the following should be included in a risk scenario to be used for risk analysis?

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

Answer: B

NEW QUESTION 213

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 217

- (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 221

- (Exam Topic 3)

Which of the following scenarios represents a threat?

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

Answer: D

NEW QUESTION 223

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 228

- (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 229

- (Exam Topic 3)

The PRIMARY reason to have risk owners assigned to entries in the risk register is to ensure:

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

Answer: A

NEW QUESTION 234

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 237

- (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 242

- (Exam Topic 3)

Which of the following is the MOST important objective of an enterprise risk management (ERM) program?

- A. To create a complete repository of risk to the organization
- B. To create a comprehensive view of critical risk to the organization
- C. To provide a bottom-up view of the most significant risk scenarios
- D. To optimize costs of managing risk scenarios in the organization

Answer: B

NEW QUESTION 244

- (Exam Topic 3)

Which of the following is the PRIMARY reason to use key control indicators (KCIs) to evaluate control operating effectiveness?

- A. To measure business exposure to risk
- B. To identify control vulnerabilities
- C. To monitor the achievement of set objectives
- D. To raise awareness of operational issues

Answer: C

NEW QUESTION 248

- (Exam Topic 3)

Which of the following roles is BEST suited to help a risk practitioner understand the impact of IT-related events on business objectives?

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

Answer: C

NEW QUESTION 249

- (Exam Topic 3)

Several newly identified risk scenarios are being integrated into an organization's risk register. The MOST appropriate risk owner would be the individual who:

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

Answer: D

NEW QUESTION 253

- (Exam Topic 3)

Reviewing historical risk events is MOST useful for which of the following processes within the risk management life cycle?

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

Answer: D

NEW QUESTION 256

- (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 260

- (Exam Topic 3)

Which of The following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?

- A. Perform a post-implementation review.
- B. Conduct user acceptance testing.
- C. Review the key performance indicators (KPIs).
- D. Interview process owners.

Answer: C

NEW QUESTION 265

- (Exam Topic 3)

Which of the following is the MOST critical element to maximize the potential for a successful security implementation?

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

Answer: C

NEW QUESTION 270

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 273

- (Exam Topic 3)

Which of the following is the MOST important reason to link an effective key control indicator (KCI) to relevant key risk indicators (KRIs)?

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

Answer: A

NEW QUESTION 274

- (Exam Topic 3)

Which of the following is the BEST Key control indicator KCO to monitor the effectiveness of patch management?

- A. Percentage of legacy servers out of support
- B. Percentage of servers receiving automata patches
- C. Number of unremediated vulnerabilities
- D. Number of intrusion attempts

Answer: D

NEW QUESTION 276

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 280

- (Exam Topic 3)

While reviewing the risk register, a risk practitioner notices that different business units have significant variances in inherent risk for the same risk scenario. Which of the following is the BEST course of action?

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

Answer: B

NEW QUESTION 284

- (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 289

- (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 291

- (Exam Topic 3)

Which of the following would BEST assist in reconstructing the sequence of events following a security incident across multiple IT systems in the organization's network?

- A. Network monitoring infrastructure
- B. Centralized vulnerability management
- C. Incident management process
- D. Centralized log management

Answer: D

NEW QUESTION 293

- (Exam Topic 3)

Which of the following would present the MOST significant risk to an organization when updating the incident response plan?

- A. Obsolete response documentation
- B. Increased stakeholder turnover
- C. Failure to audit third-party providers
- D. Undefined assignment of responsibility

Answer: D

NEW QUESTION 297

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 301

- (Exam Topic 3)

Which of the following is the BEST way to mitigate the risk to IT infrastructure availability?

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

Answer: D

NEW QUESTION 306

- (Exam Topic 3)

Which of the following practices MOST effectively safeguards the processing of personal data?

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

Answer: B

NEW QUESTION 308

- (Exam Topic 3)

Which of the following is the BEST control to detect an advanced persistent threat (APT)?

- A. Utilizing antivirus systems and firewalls
- B. Conducting regular penetration tests
- C. Monitoring social media activities
- D. Implementing automated log monitoring

Answer: D

NEW QUESTION 310

- (Exam Topic 3)

Which of the following should be management's PRIMARY consideration when approving risk response action plans?

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

Answer: C

NEW QUESTION 313

- (Exam Topic 3)

Key risk indicators (KRIs) are MOST useful during which of the following risk management phases?

- A. Monitoring
- B. Analysis
- C. Identification

D. Response selection

Answer: A

NEW QUESTION 314

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 317

- (Exam Topic 3)

Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

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

Answer: B

NEW QUESTION 321

- (Exam Topic 3)

Which of the following is necessary to enable an IT risk register to be consolidated with the rest of the organization's risk register?

- A. Risk taxonomy
- B. Risk response
- C. Risk appetite
- D. Risk ranking

Answer: A

NEW QUESTION 324

- (Exam Topic 3)

When reviewing a business continuity plan (BCP), which of the following would be the MOST significant deficiency?

- A. BCP testing is not in conjunction with the disaster recovery plan (DRP)
- B. Recovery time objectives (RTOs) do not meet business requirements.
- C. BCP is often tested using the walk-through method.
- D. Each business location has separate, inconsistent BCPs.

Answer: B

NEW QUESTION 327

- (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 330

- (Exam Topic 3)

Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

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

Answer: B

NEW QUESTION 331

- (Exam Topic 3)

Which of the following is the BEST evidence of an effective risk treatment plan?

- A. The inherent risk is below the asset residual risk.

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

Answer: B

NEW QUESTION 332

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 336

- (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 339

- (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 341

- (Exam Topic 3)

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

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

Answer: B

NEW QUESTION 345

- (Exam Topic 3)

Which of the following is the MOST important consideration when sharing risk management updates with executive management?

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

Answer: D

NEW QUESTION 346

- (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 350

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 354

- (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 358

- (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 361

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 363

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 367

- (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 372

- (Exam Topic 3)

Which of the following is MOST important to the successful development of IT risk scenarios?

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

Answer: C

NEW QUESTION 375

- (Exam Topic 3)

Which of the following would be MOST useful to senior management when determining an appropriate risk response?

- A. A comparison of current risk levels with established tolerance
- B. A comparison of cost variance with defined response strategies
- C. A comparison of current risk levels with estimated inherent risk levels
- D. A comparison of accepted risk scenarios associated with regulatory compliance

Answer: A

NEW QUESTION 380

- (Exam Topic 3)

Which of the following BEST facilitates the alignment of IT risk management with enterprise risk management (ERM)?

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

Answer: C

NEW QUESTION 385

- (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 390

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 391

- (Exam Topic 3)

The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

- A. stakeholder risk tolerance.
- B. benchmarking criteria.
- C. suppliers used by the organization.
- D. the control environment.

Answer: D

NEW QUESTION 393

- (Exam Topic 3)

Which of The following is the MOST comprehensive input to the risk assessment process specific to the effects of system downtime?

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

Answer: C

NEW QUESTION 396

- (Exam Topic 3)

Which of the following should be a risk practitioner's PRIMARY focus when tasked with ensuring organization records are being retained for a sufficient period of time to meet legal obligations?

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

Answer:

B

NEW QUESTION 398

- (Exam Topic 3)

Which of the following is the GREATEST advantage of implementing a risk management program?

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

Answer: A

NEW QUESTION 402

- (Exam Topic 3)

Which of the following BEST enables an organization to determine whether external emerging risk factors will impact the organization's risk profile?

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

Answer: D

NEW QUESTION 406

- (Exam Topic 3)

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

- 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 410

- (Exam Topic 3)

Which of the following would be MOST helpful when communicating roles associated with the IT risk management process?

- A. Skills matrix
- B. Job descriptions
- C. RACI chart
- D. Organizational chart

Answer: A

NEW QUESTION 412

- (Exam Topic 3)

Who is BEST suited to determine whether a new control properly mitigates data loss risk within a system?

- A. Data owner
- B. Control owner
- C. Risk owner
- D. System owner

Answer: B

NEW QUESTION 414

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 416

- (Exam Topic 3)

To help identify high-risk situations, an organization should:

- A. continuously monitor the environment.
- B. develop key performance indicators (KPIs).
- C. maintain a risk matrix.

D. maintain a risk register.

Answer: A

NEW QUESTION 418

- (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 422

- (Exam Topic 3)

A deficient control has been identified which could result in great harm to an organization should a low frequency threat event occur. When communicating the associated risk to senior management the risk practitioner should explain:

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

Answer: A

NEW QUESTION 424

- (Exam Topic 3)

Which of the following controls BEST helps to ensure that transaction data reaches its destination?

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

Answer: B

NEW QUESTION 425

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 427

- (Exam Topic 4)

Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

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

Answer: A

NEW QUESTION 430

- (Exam Topic 4)

Which of the following situations presents the GREATEST challenge to creating a comprehensive IT risk profile of an organization?

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

Answer: D

NEW QUESTION 432

- (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 436

- (Exam Topic 4)

Which of the following BEST balances the costs and benefits of managing IT risk*?

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

Answer: A

NEW QUESTION 437

- (Exam Topic 4)

Which of the following is MOST helpful in defining an early-warning threshold associated with insufficient network bandwidth"

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

Answer: A

NEW QUESTION 440

- (Exam Topic 4)

Which of the following is MOST helpful to understand the consequences of an IT risk event?

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

Answer: B

NEW QUESTION 445

- (Exam Topic 4)

An information security audit identified a risk resulting from the failure of an automated control Who is responsible for ensuring the risk register is updated accordingly?

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

Answer: A

NEW QUESTION 447

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 448

- (Exam Topic 4)

An organization has completed a risk assessment of one of its service providers. Who should be accountable for ensuring that risk responses are implemented?

- A. IT risk practitioner
- B. Third -partf3curity team
- C. The relationship owner
- D. Legal representation of the business

Answer: C

NEW QUESTION 449

- (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 451

- (Exam Topic 4)

An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

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

Answer: A

NEW QUESTION 456

- (Exam Topic 4)

Which of the following would BEST facilitate the implementation of data classification requirements?

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

Answer: B

NEW QUESTION 457

- (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 462

- (Exam Topic 4)

A recent vulnerability assessment of a web-facing application revealed several weaknesses. Which of the following should be done NEXT to determine the risk exposure?

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

Answer: B

NEW QUESTION 463

- (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 appetite

Answer: B

NEW QUESTION 467

- (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 471

- (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 474

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 478

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 482

- (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 483

- (Exam Topic 4)

Which of the following potential scenarios associated with the implementation of a new database technology presents the GREATEST risk to an organization?

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

Answer: B

NEW QUESTION 486

- (Exam Topic 4)

During an acquisition, which of the following would provide the MOST useful input to the parent company's risk practitioner when developing risk scenarios for the post-acquisition phase?

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

Answer: C

NEW QUESTION 488

- (Exam Topic 4)

An incentive program is MOST likely implemented to manage the risk associated with loss of which organizational asset?

- A. Employees
- B. Data
- C. Reputation
- D. Customer lists

Answer: A

NEW QUESTION 492

- (Exam Topic 4)

The PRIMARY objective of collecting information and reviewing documentation when performing periodic risk analysis should be to:

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

Answer: D

NEW QUESTION 493

- (Exam Topic 4)

Following an acquisition, the acquiring company's risk practitioner has been asked to update the organization's IT risk profile What is the MOST important information to review from the acquired company to facilitate this task?

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

Answer: C

NEW QUESTION 498

- (Exam Topic 4)

Which of the following will BEST help to ensure key risk indicators (KRIs) provide value to risk owners?

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

Answer: B

NEW QUESTION 500

- (Exam Topic 4)

Which of the following is the BEST key performance indicator (KPI) to measure how effectively risk management practices are embedded in the project management office (PMO)?

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

Answer: C

NEW QUESTION 503

- (Exam Topic 4)

Which of the following is the MOST effective way to identify an application backdoor prior to implementation'?

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

Answer: B

NEW QUESTION 507

- (Exam Topic 4)

The MAIN reason for prioritizing IT risk responses is to enable an organization to:

- A. determine the risk appetite.
- B. determine the budget.
- C. define key performance indicators (KPIs).
- D. optimize resource utilization.

Answer: C

NEW QUESTION 512

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 517

- (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 522

- (Exam Topic 4)

An organization is concerned that its employees may be unintentionally disclosing data through the use of social media sites. Which of the following will MOST effectively mitigate this risk?

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

Answer: C

NEW QUESTION 523

- (Exam Topic 4)

Which of the following is the MOST important reason to validate that risk responses have been executed as outlined in the risk response plan?

- A. To ensure completion of the risk assessment cycle
- B. To ensure controls are operating effectively
- C. To ensure residual risk is at an acceptable level
- D. To ensure control costs do not exceed benefits

Answer: A

NEW QUESTION 528

- (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 533

- (Exam Topic 4)

Which of the following is the PRIMARY objective of risk management?

- A. Identify and analyze risk.
- B. Achieve business objectives
- C. Minimize business disruptions.
- D. Identify threats and vulnerabilities.

Answer: B

NEW QUESTION 535

- (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 537

- (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 541

- (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 546

- (Exam Topic 4)

The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

- A. data logging and monitoring
- B. data mining and analytics
- C. data classification and labeling
- D. data retention and destruction

Answer: C

NEW QUESTION 547

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 552

- (Exam Topic 4)

Which of the following is the PRIMARY reason for an organization to include an acceptable use banner when users log in?

- A. To reduce the likelihood of insider threat
- B. To eliminate the possibility of insider threat
- C. To enable rapid discovery of insider threat
- D. To reduce the impact of insider threat

Answer: A

NEW QUESTION 556

- (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 557

- (Exam Topic 4)

Who is BEST suited to provide objective input when updating residual risk to reflect the results of control effectiveness?

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

Answer: C

NEW QUESTION 560

- (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 561

- (Exam Topic 4)

Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

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

Answer: C

NEW QUESTION 562

- (Exam Topic 4)

Which of the following is the BEST control to minimize the risk associated with scope creep in software development?

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

Answer: A

NEW QUESTION 566

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 567

- (Exam Topic 4)

Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

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

Answer: A

NEW QUESTION 568

- (Exam Topic 4)

When developing risk scenario using a list of generic scenarios based on industry best practices, it is MOST imported to:

- A. Assess generic risk scenarios with business users.
- B. Validate the generic risk scenarios for relevance.
- C. Select the maximum possible risk scenarios from the list.
- D. Identify common threats causing generic risk scenarios

Answer: B

NEW QUESTION 572

- (Exam Topic 4)

An organization recently configured a new business division Which of the following is MOST likely to be affected?

- A. Risk profile
- B. Risk culture
- C. Risk appetite
- D. Risk tolerance

Answer: A

NEW QUESTION 576

- (Exam Topic 4)

An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention. The business owner challenges whether the situation is worth remediating. Which of the following is the risk manager's BEST response?

- A. Identify the regulatory bodies that may highlight this gap
- B. Highlight news articles about data breaches
- C. Evaluate the risk as a measure of probable loss
- D. Verify if competitors comply with a similar policy

Answer: B

NEW QUESTION 577

- (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 579

- (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 584

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 587

- (Exam Topic 4)

When defining thresholds for control key performance indicators (KPIs), it is MOST helpful to align:

- A. information risk assessments with enterprise risk assessments.
- B. key risk indicators (KRIs) with risk appetite of the business.
- C. the control key performance indicators (KPIs) with audit findings.
- D. control performance with risk tolerance of business owners.

Answer: B

NEW QUESTION 590

- (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 591

- (Exam Topic 4)

Which of the following is the MOST important consideration when communicating the risk associated with technology end-of-life to business owners?

- A. Cost and benefit
- B. Security and availability
- C. Maintainability and reliability
- D. Performance and productivity

Answer: A

NEW QUESTION 592

- (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 596

- (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 601

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 603

- (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 607

- (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 609

- (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 611

- (Exam Topic 4)

The MAJOR reason to classify information assets is

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

Answer: C

NEW QUESTION 614

- (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 615

- (Exam Topic 4)

Which of the following BEST reduces the risk associated with the theft of a laptop containing sensitive information?

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

Answer: B

NEW QUESTION 617

- (Exam Topic 4)

Which of the following is the BEST way to determine whether system settings are in alignment with control baselines?

- A. Configuration validation
- B. Control attestation
- C. Penetration testing
- D. Internal audit review

Answer: A

NEW QUESTION 619

- (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 621

- (Exam Topic 4)

Which of the following is MOST helpful in providing a high-level overview of current IT risk severity*?

- A. Risk mitigation plans
- B. heat map
- C. Risk appetite statement
- D. Key risk indicators (KRIs)

Answer: B

NEW QUESTION 625

- (Exam Topic 4)

When creating a separate IT risk register for a large organization, which of the following is MOST important to consider with regard to the existing corporate risk 'register'?

- A. Leveraging business risk professionals
- B. Relying on generic IT risk scenarios
- C. Describing IT risk in business terms
- D. Using a common risk taxonomy

Answer: D

NEW QUESTION 626

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 629

- (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 632

- (Exam Topic 4)

Which of the following is the PRIMARY objective of establishing an organization's risk tolerance and appetite?

- A. To align with board reporting requirements
- B. To assist management in decision making
- C. To create organization-wide risk awareness
- D. To minimize risk mitigation efforts

Answer: B

NEW QUESTION 634

- (Exam Topic 4)

An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

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

Answer: A

NEW QUESTION 638

- (Exam Topic 4)

Which of the following is MOST important to include when reporting the effectiveness of risk management to senior management?

- A. Changes in the organization's risk appetite and risk tolerance levels
- B. Impact due to changes in external and internal risk factors
- C. Changes in residual risk levels against acceptable levels
- D. Gaps in best practices and implemented controls across the industry

Answer: C

NEW QUESTION 640

- (Exam Topic 4)

Which of the following is MOST important to update when an organization's risk appetite changes?

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

Answer: A

NEW QUESTION 644

- (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 646

- (Exam Topic 4)

After an annual risk assessment is completed, which of the following would be MOST important to communicate to stakeholders?

- A. A decrease in threats
- B. A change in the risk profile
- C. An increase in reported vulnerabilities
- D. An increase in identified risk scenarios

Answer: B

NEW QUESTION 650

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 653

- (Exam Topic 4)

Who is the BEST person to manage employee personal data?

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

Answer: A

NEW QUESTION 657

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 658

- (Exam Topic 4)

An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:

- A. a recognized industry control framework
- B. guidance provided by the external auditor
- C. the service provider's existing controls
- D. The organization's specific control requirements

Answer: D

NEW QUESTION 661

- (Exam Topic 4)

It is MOST important that security controls for a new system be documented in:

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

Answer: C

NEW QUESTION 663

- (Exam Topic 4)

Which of the following is the GREATEST benefit of identifying appropriate risk owners?

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

Answer: A

NEW QUESTION 668

- (Exam Topic 4)

Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

- A. To identify gaps in data protection controls
- B. To develop a customer notification plan
- C. To identify personally identifiable information (PII)
- D. To determine gaps in data identification processes

Answer: A

NEW QUESTION 671

- (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 675

- (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 680

- (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 685

- (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 690

- (Exam Topic 4)

A bank recently incorporated Blockchain technology with the potential to impact known risk within the organization. Which of the following is the risk practitioner's BEST course of action?

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

Answer: B

NEW QUESTION 693

- (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 696

- (Exam Topic 4)

A newly incorporated enterprise needs to secure its information assets From a governance perspective which of the following should be done FIRST?

- A. Define information retention requirements and policies
- B. Provide information security awareness training
- C. Establish security management processes and procedures
- D. Establish an inventory of information assets

Answer: D

NEW QUESTION 699

- (Exam Topic 4)

An internal audit report reveals that a legacy system is no longer supported Which of the following is the risk practitioner's MOST important action before recommending a risk response'

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

Answer: B

NEW QUESTION 700

- (Exam Topic 4)

Which of the following is MOST important when determining risk appetite?

- A. Assessing regulatory requirements
- B. Benchmarking against industry standards
- C. Gaining management consensus
- D. Identifying risk tolerance

Answer: C

NEW QUESTION 704

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 709

- (Exam Topic 4)

Which of the following is the MOST important benefit of reporting risk assessment results to senior management?

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

Answer: D

NEW QUESTION 712

- (Exam Topic 4)

it was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern1?

- A. The underutilization of the replicated 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 715

- (Exam Topic 3)

Which of the following will be the GREATEST concern when assessing the risk profile of an organization?

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

Answer: A

NEW QUESTION 718

- (Exam Topic 3)

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

- A. Potential loss to tie 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 721

- (Exam Topic 3)

Which of the following should be implemented to BEST mitigate the risk associated with infrastructure updates?

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

Answer: C

NEW QUESTION 724

- (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 726

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 730

- (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 734

- (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 738

- (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 740

- (Exam Topic 3)

Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

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

Answer: A

NEW QUESTION 743

- (Exam Topic 3)

What is the PRIMARY purpose of a business impact analysis (BIA)?

- A. To determine the likelihood and impact of threats to business operations
- B. To identify important business processes in the organization
- C. To estimate resource requirements for related business processes
- D. To evaluate the priority of business operations in case of disruption

Answer: D

NEW QUESTION 744

- (Exam Topic 3)

Which of the following practices BEST mitigates risk related to enterprise-wide ethical decision making in a multi-national organization?

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

Answer: A

NEW QUESTION 745

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 749

- (Exam Topic 3)

An organization's risk register contains a large volume of risk scenarios that senior management considers overwhelming. Which of the following would BEST help to improve the risk register?

- A. Analyzing the residual risk components
- B. Performing risk prioritization
- C. Validating the risk appetite level
- D. Conducting a risk assessment

Answer: D

NEW QUESTION 753

- (Exam Topic 3)

Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

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

Answer: A

NEW QUESTION 758

- (Exam Topic 3)

Which of the following would be the GREATEST challenge when implementing a corporate risk framework for a global organization?

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

Answer: A

NEW QUESTION 761

- (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 766

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 771

- (Exam Topic 3)

The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

- A. availability of fault tolerant software.
- B. strategic plan for business growth.
- C. vulnerability scan results of critical systems.
- D. redundancy of technical infrastructure.

Answer: D

NEW QUESTION 774

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 777

- (Exam Topic 3)

A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

- A. Monitor processes to ensure recent updates are being followed.
- B. Communicate to those who test and promote changes.
- C. Conduct a cost-benefit analysis to justify the cost of the control.
- D. Assess the maturity of the change management process.

Answer: A

NEW QUESTION 782

- (Exam Topic 3)

Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

- A. Occurrences of specific events
- B. A performance measurement
- C. The risk tolerance level

D. Risk scenarios

Answer: C

NEW QUESTION 785

- (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 788

- (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 793

- (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 797

- (Exam Topic 3)

The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

- A. accounts without documented approval
- B. user accounts with default passwords
- C. active accounts belonging to former personnel
- D. accounts with dormant activity.

Answer: A

NEW QUESTION 798

- (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 801

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 802

- (Exam Topic 3)

Which of the following BEST mitigates the risk of sensitive personal data leakage from a software development environment?

- A. Tokenized personal data only in test environments

- B. Data loss prevention tools (DLP) installed in passive mode
- C. Anonymized personal data in non-production environments
- D. Multi-factor authentication for access to non-production environments

Answer: C

NEW QUESTION 807

- (Exam Topic 3)

Which of the following BEST indicates the efficiency of a process for granting access privileges?

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

Answer: C

NEW QUESTION 808

- (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 809

- (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 810

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 815

- (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 817

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 818

- (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 820

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 821

- (Exam Topic 3)

A risk practitioner has become aware of production data being used in a test environment. Which of the following should be the practitioner's PRIMARY concern?

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

Answer: A

NEW QUESTION 823

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 825

- (Exam Topic 3)

To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:

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

Answer: A

NEW QUESTION 830

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 831

- (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 834

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 838

- (Exam Topic 3)

Which of the following BEST protects an organization against breaches when using a software as a service (SaaS) application?

- A. Control self-assessment (CSA)
- B. Security information and event management (SIEM) solutions
- C. Data privacy impact assessment (DPIA)
- D. Data loss prevention (DLP) tools

Answer: B

NEW QUESTION 841

- (Exam Topic 3)

Which of the following is the FIRST step when conducting a business impact analysis (BIA)?

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

Answer: A

NEW QUESTION 845

- (Exam Topic 3)

The MOST important consideration when selecting a control to mitigate an identified risk is whether:

- A. the cost of control exceeds the mitigation value
- B. there are sufficient internal resources to implement the control
- C. the mitigation measures create compounding effects
- D. the control eliminates the risk

Answer: A

NEW QUESTION 847

- (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 852

- (Exam Topic 3)

Which of the following MUST be updated to maintain an IT risk register?

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

Answer: C

NEW QUESTION 856

- (Exam Topic 3)

While reviewing an organization's monthly change management metrics, a risk practitioner notes that the number of emergency changes has increased substantially. Which of the following would be the BEST approach for the risk practitioner to take?

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

Answer: C

NEW QUESTION 857

- (Exam Topic 3)

Management has required information security awareness training to reduce the risk associated with credential compromise. What is the BEST way to assess the effectiveness of the training?

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

Answer: A

NEW QUESTION 860

- (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 865

- (Exam Topic 3)

Accountability for a particular risk is BEST represented in a:

- A. risk register
- B. risk catalog
- C. risk scenario
- D. RACI matrix

Answer: D

NEW QUESTION 869

- (Exam Topic 3)

Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?

- A. Piloting courses with focus groups
- B. Using reputable third-party training programs
- C. Reviewing content with senior management
- D. Creating modules for targeted audiences

Answer: D

NEW QUESTION 873

- (Exam Topic 2)

An organization with a large number of applications wants to establish a security risk assessment program. Which of the following would provide the MOST useful information when determining the frequency of risk assessments?

- A. Feedback from end users
- B. Results of a benchmark analysis
- C. Recommendations from internal audit
- D. Prioritization from business owners

Answer: D

NEW QUESTION 874

- (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 875

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CRISC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CRISC Product From:

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

Money Back Guarantee

CRISC Practice Exam Features:

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