

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)

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

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

Answer: C

NEW QUESTION 3

- (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 4

- (Exam Topic 4)

Which of the following should be the GREATEST concern to a risk practitioner when process documentation is incomplete?

- A. Inability to allocate resources efficiently
- B. Inability to identify the risk owner
- C. Inability to complete the risk register
- D. Inability to identify process experts

Answer: B

NEW QUESTION 5

- (Exam Topic 4)

A global company's business continuity plan (BCP) requires the transfer of its customer information.... event of a disaster. Which of the following should be the MOST important risk consideration?

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

Answer: B

NEW QUESTION 6

- (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 7

- (Exam Topic 4)

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

- A. mitigated

- B. deferred
- C. accepted.
- D. transferred

Answer: C

NEW QUESTION 8

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 9

- (Exam Topic 4)

Which of the following would provide the MOST useful input when evaluating the appropriateness of risk responses?

- A. Incident reports
- B. Cost-benefit analysis
- C. Risk tolerance
- D. Control objectives

Answer: B

NEW QUESTION 10

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 4)

Which of the following is the MOST effective way to promote organization-wide awareness of data security in response to an increase in regulatory penalties for data leakage?

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

Answer: B

NEW QUESTION 13

- (Exam Topic 4)

Which of the following is the MOST important information to cover a business continuity awareness training program for all employees of the organization?

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

Answer: C

NEW QUESTION 14

- (Exam Topic 4)

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 16

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 17

- (Exam Topic 4)

Risk appetite should be PRIMARILY driven by which of the following?

- A. Enterprise security architecture roadmap
- B. Stakeholder requirements
- C. Legal and regulatory requirements
- D. Business impact analysis (BIA)

Answer: B

NEW QUESTION 22

- (Exam Topic 4)

Which of the following would be of MOST concern to a risk practitioner reviewing risk action plans for documented IT risk scenarios?

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

Answer: B

NEW QUESTION 27

- (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 31

- (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 36

- (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 39

- (Exam Topic 4)

Which of the following, who should be PRIMARILY responsible for performing user entitlement reviews?

- A. IT security manager
- B. IT personnel
- C. Data custodian
- D. Data owner

Answer: D

NEW QUESTION 41

- (Exam Topic 4)

After undertaking a risk assessment of a production system, the MOST appropriate action is for the risk manager to

- A. recommend a program that minimizes the concerns of that production system.
- B. inform the process owner of the concerns and propose measures to reduce them.
- C. inform the IT manager of the concerns and propose measures to reduce them.
- D. inform the development team of the concerns and together formulate risk reduction measures.

Answer: B

NEW QUESTION 45

- (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 50

- (Exam Topic 4)

Which of the following would provide the BEST evidence of an effective internal control environment/?

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

Answer: D

NEW QUESTION 53

- (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 55

- (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 56

- (Exam Topic 4)

A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?

- A. Collaborate with the risk owner to determine the risk response plan.
- B. Document the gap in the risk register and report to senior management.
- C. Include a right to audit clause in the service provider contract.
- D. Advise the risk owner to accept the risk.

Answer: C

NEW QUESTION 57

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 58

- (Exam Topic 4)

An organization has asked an IT risk practitioner to conduct an operational risk assessment on an initiative to outsource the organization's customer service operations overseas. Which of the following would MOST significantly impact management's decision?

- A. Time zone difference of the outsourcing location
- B. Ongoing financial viability of the outsourcing company
- C. Cross-border information transfer restrictions in the outsourcing country
- D. Historical network latency between the organization and outsourcing location

Answer: C

NEW QUESTION 63

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 64

- (Exam Topic 4)

Which of the following is the MOST important consideration when developing risk strategies?

- A. Organization's industry sector
- B. Long-term organizational goals
- C. Concerns of the business process owners
- D. History of risk events

Answer: B

NEW QUESTION 69

- (Exam Topic 4)

Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

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

Answer: A

NEW QUESTION 74

- (Exam Topic 4)

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

- 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 76

- (Exam Topic 4)

A multinational organization is considering implementing standard background checks to all new employees. A KEY concern regarding this approach

- A. fail to identify all relevant issues.
- B. be too costly
- C. violate laws in other countries
- D. be too time consuming

Answer: C

NEW QUESTION 79

- (Exam Topic 3)

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

- A. Sustained financial loss
- B. Cost of remediation efforts

- C. Duration of service outage
- D. Average time to recovery

Answer: A

NEW QUESTION 83

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 84

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 88

- (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 89

- (Exam Topic 4)

Which of the following is MOST important to consider before determining a response to a vulnerability?

- A. The likelihood and impact of threat events
- B. The cost to implement the risk response
- C. Lack of data to measure threat events
- D. Monetary value of the asset

Answer: C

NEW QUESTION 91

- (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 94

- (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 96

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 99

- (Exam Topic 3)

Which of the following provides the BEST evidence that a selected risk treatment plan is effective?

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

Answer: D

NEW QUESTION 100

- (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 103

- (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 107

- (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 108

- (Exam Topic 3)

Which of the following can be concluded by analyzing the latest vulnerability report for the IT infrastructure?

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

Answer: C

NEW QUESTION 112

- (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 113

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 115

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 119

- (Exam Topic 3)

Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

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

Answer: C

NEW QUESTION 123

- (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 127

- (Exam Topic 3)

Which of the following should be the FIRST consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected?

- A. Informed consent
- B. Cross border controls
- C. Business impact analysis (BIA)
- D. Data breach protection

Answer: A

NEW QUESTION 132

- (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 135

- (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 136

- (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 141

- (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 145

- (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 149

- (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 151

- (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 156

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 157

- (Exam Topic 3)

An organization's chief technology officer (CTO) has decided to accept the risk associated with the potential loss from a denial-of-service (DoS) attack. In this situation, the risk practitioner's BEST course of action is to:

- A. identify key risk indicators (KRIs) for ongoing monitoring

- B. validate the CTO's decision with the business process owner
- C. update the risk register with the selected risk response
- D. recommend that the CTO revisit the risk acceptance decision.

Answer: A

NEW QUESTION 158

- (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 163

- (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 164

- (Exam Topic 3)

The MOST important reason for implementing change control procedures is to ensure:

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

Answer: A

NEW QUESTION 165

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 170

- (Exam Topic 3)

Which of the following is the BEST indication of a mature organizational risk culture?

- A. Corporate risk appetite is communicated to staff members.
- B. Risk owners understand and accept accountability for risk.
- C. Risk policy has been published and acknowledged by employees.
- D. Management encourages the reporting of policy breaches.

Answer: B

NEW QUESTION 173

- (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 177

- (Exam Topic 3)

Determining if organizational risk is tolerable requires:

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

Answer: D

NEW QUESTION 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 182

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 184

- (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 189

- (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 195

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 198

- (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 203

- (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 208

- (Exam Topic 3)

When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs?

- A. Risk management
- B. Change management
- C. Problem management
- D. Quality management

Answer: B

NEW QUESTION 209

- (Exam Topic 3)

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

- A. detected incidents.
- B. residual risk.
- C. vulnerabilities.
- D. inherent risk.

Answer: D

NEW QUESTION 210

- (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 212

- (Exam Topic 3)

Which of the following BEST enables the identification of trends in risk levels?

- A. Correlation between risk levels and key risk indicators (KRIs) is positive.
- B. Measurements for key risk indicators (KRIs) are repeatable
- C. Quantitative measurements are used for key risk indicators (KRIs).
- D. Qualitative definitions for key risk indicators (KRIs) are used.

Answer: B

NEW QUESTION 213

- (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 216

- (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 221

- (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 226

- (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 227

- (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 232

- (Exam Topic 3)

Which of the following key control indicators (KCIs) BEST indicates whether security requirements are identified and managed throughout a project life cycle?

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

Answer: A

NEW QUESTION 236

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 240

- (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 243

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 244

- (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 246

- (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 247

- (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 248

- (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 253

- (Exam Topic 3)

To reduce costs, an organization is combining the second and third lines of defense in a new department that reports to a recently appointed C-level executive. Which of the following is the GREATEST concern with this situation?

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

Answer: B

NEW QUESTION 257

- (Exam Topic 3)

Which of the following BEST indicates the risk appetite and tolerance level (or the risk associated with business interruption caused by IT system failures)?

- A. Mean time to recover (MTTR)

- B. IT system criticality classification
- C. Incident management service level agreement (SLA)
- D. Recovery time objective (RTO)

Answer: D

NEW QUESTION 260

- (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 264

- (Exam Topic 3)

Which of the following approaches to bring your own device (BYOD) service delivery provides the BEST protection from data loss?

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

Answer: D

NEW QUESTION 269

- (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 273

- (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 275

- (Exam Topic 3)

The PRIMARY objective of a risk identification process is to:

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

Answer: B

NEW QUESTION 276

- (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 280

- (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 283

- (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 287

- (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 289

- (Exam Topic 3)

What should be the PRIMARY driver for periodically reviewing and adjusting key risk indicators (KRIs)?

- A. Risk impact
- B. Risk likelihood
- C. Risk appropriate
- D. Control self-assessments (CSAs)

Answer: B

NEW QUESTION 292

- (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 293

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 298

- (Exam Topic 3)

When formulating a social media policy to address information leakage, which of the following is the MOST important concern to address?

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

Answer: A

NEW QUESTION 303

- (Exam Topic 3)

Which of the following should be the PRIMARY focus of an IT risk awareness program?

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

Answer: B

NEW QUESTION 306

- (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 311

- (Exam Topic 3)

Which of the following risk management practices BEST facilitates the incorporation of IT risk scenarios into the enterprise-wide risk register?

- A. Key risk indicators (KRIs) are developed for key IT risk scenarios
- B. IT risk scenarios are assessed by the enterprise risk management team
- C. Risk appetites for IT risk scenarios are approved by key business stakeholders.
- D. IT risk scenarios are developed in the context of organizational objectives.

Answer: D

NEW QUESTION 312

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 316

- (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 318

- (Exam Topic 3)

Which of the following controls BEST enables an organization to ensure a complete and accurate IT asset inventory?

- A. Prohibiting the use of personal devices for business
- B. Performing network scanning for unknown devices
- C. Requesting an asset list from business owners
- D. Documenting asset configuration baselines

Answer: B

NEW QUESTION 319

- (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 323

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 325

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 327

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 330

- (Exam Topic 3)

An organization uses a vendor to destroy hard drives. Which of the following would BEST reduce the risk of data leakage?

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

Answer: B

NEW QUESTION 331

- (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 336

- (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 337

- (Exam Topic 3)

Which of the following is the MOST effective control to address the risk associated with compromising data privacy within the cloud?

- A. Establish baseline security configurations with the cloud service provider.
- B. Require the cloud provider to disclose past data privacy breaches.
- C. Ensure the cloud service provider performs an annual risk assessment.

D. Specify cloud service provider liability for data privacy breaches in the contract

Answer: D

NEW QUESTION 342

- (Exam Topic 3)

Print jobs containing confidential information are sent to a shared network printer located in a secure room. Which of the following is the BEST control to prevent the inappropriate disclosure of confidential information?

- A. Requiring a printer access code for each user
- B. Using physical controls to access the printer room
- C. Using video surveillance in the printer room
- D. Ensuring printer parameters are properly configured

Answer: A

NEW QUESTION 347

- (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 351

- (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 356

- (Exam Topic 3)

Which of The following should be the FIRST step when a company is made aware of new regulatory requirements impacting IT?

- A. Perform a gap analysis.
- B. Prioritize impact to the business units.
- C. Perform a risk assessment.
- D. Review the risk tolerance and appetite.

Answer: C

NEW QUESTION 360

- (Exam Topic 3)

Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?

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

Answer: A

NEW QUESTION 362

- (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 364

- (Exam Topic 3)

All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the

BEST course of action would be to:

- A. select a provider to standardize the disaster recovery plans.
- B. outsource disaster recovery to an external provider.
- C. centralize the risk response function at the enterprise level.
- D. evaluate opportunities to combine disaster recovery plans.

Answer: D

NEW QUESTION 368

- (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 372

- (Exam Topic 4)

Which of the following would provide the MOST helpful input to develop risk scenarios associated with hosting an organization's key IT applications in a cloud environment?

- A. Reviewing the results of independent audits
- B. Performing a site visit to the cloud provider's data center
- C. Performing a due diligence review
- D. Conducting a risk workshop with key stakeholders

Answer: D

NEW QUESTION 377

- (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 378

- (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 380

- (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 385

- (Exam Topic 4)

An organization has an approved bring your own device (BYOD) policy. Which of the following would BEST mitigate the security risk associated with the inappropriate use of enterprise applications on the devices?

- A. Periodically review application on BYOD devices
- B. Include BYOD in organizational awareness programs
- C. Implement BYOD mobile device management (MDM) controls.
- D. Enable a remote wee capability for BYOD devices

Answer: C

NEW QUESTION 389

- (Exam Topic 4)

Which of the following will BEST help to ensure the continued effectiveness of the IT risk management function within an organization experiencing high employee turnover?

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

Answer: B

NEW QUESTION 392

- (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 -part3security team
- C. The relationship owner
- D. Legal representation of the business

Answer: C

NEW QUESTION 393

- (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 394

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 397

- (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 400

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 402

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 405

- (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 406

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 411

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 412

- (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 416

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 418

- (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 420

- (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 425

- (Exam Topic 4)

An organization is planning to move its application infrastructure from on-premises to the cloud. Which of the following is the BEST course of the action to address the risk associated with data transfer if the relationship is terminated with the vendor?

- A. Meet with the business leaders to ensure the classification of their transferred data is in place
- B. Ensure the language in the contract explicitly states who is accountable for each step of the data transfer process
- C. Collect requirements for the environment to ensure the infrastructure as a service (IaaS) is configured appropriately.
- D. Work closely with the information security officer to ensure the company has the proper security controls in place.

Answer: B

NEW QUESTION 430

- (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 433

- (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 436

- (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 441

- (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 443

- (Exam Topic 4)

Which of the following BEST enables effective IT control implementation?

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

Answer: B

NEW QUESTION 446

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 448

- (Exam Topic 4)

Which of the following is the result of a realized risk scenario?

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

Answer: D

NEW QUESTION 452

- (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 455

- (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 459

- (Exam Topic 4)

Which stakeholder is MOST important to include when defining a risk profile during the selection process for a new third party application?

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

Answer: B

NEW QUESTION 462

- (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 467

- (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 472

- (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 476

- (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 478

- (Exam Topic 4)

When confirming whether implemented controls are operating effectively, which of the following is MOST important to review?

- A. Results of benchmarking studies
- B. Results of risk assessments
- C. Number of emergency change requests
- D. Maturity model

Answer: B

NEW QUESTION 481

- (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 486

- (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 489

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 493

- (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 495

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 496

- (Exam Topic 4)

Which of the following is the MOST effective way to reduce potential losses due to ongoing expense fraud?

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

Answer: A

NEW QUESTION 499

- (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 501

- (Exam Topic 4)

An organization control environment is MOST effective when:

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

Answer: B

NEW QUESTION 504

- (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 509

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 512

- (Exam Topic 4)

Who is MOST appropriate to be assigned ownership of a control

- A. The individual responsible for control operation
- B. The individual informed of the control effectiveness
- C. The individual responsible for resting the control
- D. The individual accountable for monitoring control effectiveness

Answer: D

NEW QUESTION 514

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 519

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 523

- (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 527

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 529

- (Exam Topic 4)

Which of the following is MOST important for successful incident response?

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

Answer: D

NEW QUESTION 531

- (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 532

- (Exam Topic 4)

An organization has been experiencing an increasing number of spear phishing attacks. Which of the following would be the MOST effective way to mitigate the risk associated with these attacks?

- A. Update firewall configuration
- B. Require strong password complexity
- C. implement a security awareness program
- D. Implement two-factor authentication

Answer: A

NEW QUESTION 537

- (Exam Topic 4)

Which of the following is the PRIMARY objective of maintaining an information asset inventory?

- A. To provide input to business impact analyses (BIAs)
- B. To protect information assets
- C. To facilitate risk assessments
- D. To manage information asset licensing

Answer: B

NEW QUESTION 541

- (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 546

- (Exam Topic 4)

Which of the following is the PRIMARY reason to perform periodic vendor risk assessments?

- A. To provide input to the organization's risk appetite
- B. To monitor the vendor's control effectiveness
- C. To verify the vendor's ongoing financial viability
- D. To assess the vendor's risk mitigation plans

Answer: B

NEW QUESTION 549

- (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 553

- (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 555

- (Exam Topic 4)

Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

- A. Ability to determine business impact
- B. Up-to-date knowledge on risk responses
- C. Decision-making authority for risk treatment
- D. Awareness of emerging business threats

Answer: A

NEW QUESTION 557

- (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 562

- (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 563

- (Exam Topic 4)

Which of the following is MOST important information to review when developing plans for using emerging technologies?

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

Answer: D

NEW QUESTION 568

- (Exam Topic 4)

Before assigning sensitivity levels to information it is MOST important to:

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

Answer: B

NEW QUESTION 571

- (Exam Topic 4)

Which of the following is MOST useful for measuring the existing risk management process against a desired state?

- A. Balanced scorecard
- B. Risk management framework
- C. Capability maturity model
- D. Risk scenario analysis

Answer: C

NEW QUESTION 574

- (Exam Topic 4)

A risk practitioner has established that a particular control is working as desired, but the annual cost of maintenance has increased and now exceeds the expected annual loss exposure. The result is that the control is:

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

Answer: B

NEW QUESTION 575

- (Exam Topic 4)

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

- 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 578

- (Exam Topic 4)

A risk practitioner has identified that the agreed recovery time objective (RTO) with a Software as a Service (SaaS) provider is longer than the business expectation. Which of the following is the risk practitioner's BEST course of action?

- A. Collaborate with the risk owner to determine the risk response plan.
- B. Document the gap in the risk register and report to senior management.
- C. Include a right to audit clause in the service provider contract.
- D. Advise the risk owner to accept the risk.

Answer: A

NEW QUESTION 581

- (Exam Topic 4)

Which of the following is the MOST important step to ensure regulatory requirements are adequately addressed within an organization?

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

Answer: B

NEW QUESTION 583

- (Exam Topic 4)

Who is the BEST person to the employee personal data?

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

Answer: A

NEW QUESTION 584

- (Exam Topic 4)

Which of the following should be accountable for ensuring that media containing financial information are adequately destroyed per an organization's data disposal policy?

- A. Compliance manager
- B. Data architect
- C. Data owner
- D. Chief information officer (CIO)

Answer: C

NEW QUESTION 589

- (Exam Topic 4)

Who should be responsible for determining which stakeholders need to be involved in the development of a risk scenario?

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

Answer: B

NEW QUESTION 594

- (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 end points 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 595

- (Exam Topic 4)

An IT risk threat analysis is BEST used to establish

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

D. risk ownership.

Answer: A

NEW QUESTION 600

- (Exam Topic 4)

Which of the following would present the GREATEST challenge for a risk practitioner during a merger of two organizations?

- A. Variances between organizational risk appetites
- B. Different taxonomies to categorize risk scenarios
- C. Disparate platforms for governance, risk, and compliance (GRC) systems
- D. Dissimilar organizational risk acceptance protocols

Answer: A

NEW QUESTION 605

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 609

- (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 613

- (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 614

- (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 619

- (Exam Topic 4)

Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?

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

Answer: D

NEW QUESTION 622

- (Exam Topic 4)

What should be the PRIMARY consideration related to data privacy protection when there are plans for a business initiative to make use of personal information?

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

Answer: D

NEW QUESTION 624

- (Exam Topic 4)

A segregation of duties control was found to be ineffective because it did not account for all applicable functions when evaluating access. Who is responsible for ensuring the control is designed to effectively address risk?

- A. Risk manager
- B. Control owner
- C. Control tester
- D. Risk owner

Answer: B

NEW QUESTION 629

- (Exam Topic 4)

Which of the following should be a risk practitioner's NEXT step after learning of an incident that has affected a competitor?

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

Answer: A

NEW QUESTION 633

- (Exam Topic 4)

After entering a large number of low-risk scenarios into the risk register, it is MOST important for the risk practitioner to:

- A. prepare a follow-up risk assessment.
- B. recommend acceptance of the risk scenarios.
- C. reconfirm risk tolerance levels.
- D. analyze changes to aggregate risk.

Answer: D

NEW QUESTION 635

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 638

- (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 639

- (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 643

- (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 644

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 647

- (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 650

- (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 651

- (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 655

- (Exam Topic 3)

Upon learning that the number of failed back-up attempts continually exceeds the current risk threshold, the risk practitioner should:

- A. inquire about the status of any planned corrective actions
- B. keep monitoring the situation as there is evidence that this is normal
- C. adjust the risk threshold to better reflect actual performance
- D. initiate corrective action to address the known deficiency

Answer: D

NEW QUESTION 657

- (Exam Topic 3)

Which of the following BEST supports ethical IT risk management practices?

- A. Robust organizational communication channels
- B. Mapping of key risk indicators (KRIs) to corporate strategy
- C. Capability maturity models integrated with risk management frameworks
- D. Rigorously enforced operational service level agreements (SLAs)

Answer: A

NEW QUESTION 659

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 661

- (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 666

- (Exam Topic 3)

When an organization's disaster recovery plan (DRP) has a reciprocal agreement, which of the following risk treatment options is being applied?

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

Answer: B

NEW QUESTION 670

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 672

- (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 674

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 677

- (Exam Topic 3)

Who should be PRIMARILY responsible for establishing an organization's IT risk culture?

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

Answer: B

NEW QUESTION 680

- (Exam Topic 3)

Which of the following BEST informs decision-makers about the value of a notice and consent control for the collection of personal information?

- A. A comparison of the costs of notice and consent control options
- B. Examples of regulatory fines incurred by industry peers for noncompliance
- C. A report of critical controls showing the importance of notice and consent
- D. A cost-benefit analysis of the control versus probable legal action

Answer: D

NEW QUESTION 681

- (Exam Topic 3)

An organization planning to transfer and store its customer data with an offshore cloud service provider should be PRIMARILY concerned with:

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

Answer: B

NEW QUESTION 685

- (Exam Topic 3)

Prudent business practice requires that risk appetite not exceed:

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

Answer: C

NEW QUESTION 688

- (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 689

- (Exam Topic 3)

Which of the following BEST assists in justifying an investment in automated controls?

- A. Cost-benefit analysis
- B. Alignment of investment with risk appetite
- C. Elimination of compensating controls
- D. Reduction in personnel costs

Answer: A

NEW QUESTION 690

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 694

- (Exam Topic 3)

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

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

Answer:

C

NEW QUESTION 695

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 698

- (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 703

- (Exam Topic 3)

The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

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

Answer: D

NEW QUESTION 704

- (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 705

- (Exam Topic 3)

Which of the following is the BEST indicator of an effective IT security awareness program?

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

Answer: A

NEW QUESTION 709

- (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 713

- (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 714

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 718

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 722

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 725

- (Exam Topic 3)

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 730

- (Exam Topic 3)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery test of critical business processes?

- A. Percentage of job failures identified and resolved during the recovery process
- B. Percentage of processes recovered within the recovery time and point objectives
- C. Number of current test plans and procedures
- D. Number of issues and action items resolved during the recovery test

Answer: B

NEW QUESTION 733

- (Exam Topic 3)

Which of the following BEST facilitates the mitigation of identified gaps between current and desired risk environment states?

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

Answer: A

NEW QUESTION 738

- (Exam Topic 3)

A maturity model is MOST useful to an organization when it:

- A. benchmarks against other organizations

- B. defines a qualitative measure of risk
- C. provides a reference for progress
- D. provides risk metrics.

Answer: C

NEW QUESTION 739

- (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 740

- (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 741

- (Exam Topic 3)

Which of the following is the PRIMARY reason to adopt key control indicators (KCIs) 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 744

- (Exam Topic 3)

A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:

- A. management.
- B. tolerance.
- C. culture.
- D. analysis.

Answer: C

NEW QUESTION 746

- (Exam Topic 3)

Which of the following would provide the MOST useful information to a risk owner when reviewing the progress of risk mitigation?

- A. Key audit findings
- B. Treatment plan status
- C. Performance indicators
- D. Risk scenario results

Answer: C

NEW QUESTION 751

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 754

- (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 759

- (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 760

- (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 762

- (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 767

- (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 772

- (Exam Topic 3)

The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

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

Answer: D

NEW QUESTION 775

- (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 779

- (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 783

- (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 788

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 792

- (Exam Topic 3)

Which of the following would BEST help to address the risk associated with malicious outsiders modifying application data?

- A. Multi-factor authentication
- B. Role-based access controls
- C. Activation of control audits
- D. Acceptable use policies

Answer: A

NEW QUESTION 795

- (Exam Topic 3)

An IT risk practitioner has been asked to regularly report on the overall status and effectiveness of the IT risk management program. Which of the following is MOST useful for this purpose?

- A. Balanced scorecard
- B. Capability maturity level
- C. Internal audit plan
- D. Control self-assessment (CSA)

Answer: A

NEW QUESTION 798

- (Exam Topic 3)

Which of the following scenarios presents the GREATEST risk for a global organization when implementing a data classification policy?

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

Answer: D

NEW QUESTION 802

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 804

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 809

- (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 811

- (Exam Topic 2)

Which of the following is MOST important for an organization that wants to reduce IT operational risk?

- A. Increasing senior management's understanding of IT operations
- B. Increasing the frequency of data backups
- C. Minimizing complexity of IT infrastructure
- D. Decentralizing IT infrastructure

Answer: C

NEW QUESTION 813

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 814

- (Exam Topic 2)

The PRIMARY benefit of classifying information assets is that it helps to:

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

Answer: D

NEW QUESTION 815

- (Exam Topic 2)

The PRIMARY objective of The board of directors periodically reviewing the risk profile is to help ensure:

- A. the risk strategy is appropriate
- B. KRIs and KPIs are aligned
- C. performance of controls is adequate
- D. the risk monitoring process has been established

Answer: A

NEW QUESTION 820

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 821

- (Exam Topic 2)

Controls should be defined during the design phase of system development because:

- A. it is more cost-effective to determine controls in the early design phase.
- B. structured analysis techniques exclude identification of controls.
- C. structured programming techniques require that controls be designed before coding begins.
- D. technical specifications are defined during this phase.

Answer: A

NEW QUESTION 824

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 826

- (Exam Topic 2)

A risk practitioner notices that a particular key risk indicator (KRI) has remained below its established trigger point for an extended period of time. Which of the following should be done FIRST?

- A. Recommend a re-evaluation of the current threshold of the KRI.
- B. Notify management that KRIs are being effectively managed.
- C. Update the risk rating associated with the KRI in the risk register.
- D. Update the risk tolerance and risk appetite to better align to the KRI.

Answer: A

NEW QUESTION 828

- (Exam Topic 2)

An organization is making significant changes to an application. At what point should the application risk profile be updated?

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

Answer: D

NEW QUESTION 832

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 836

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 838

- (Exam Topic 2)

Which of the following MUST be assessed before considering risk treatment options for a scenario with significant impact?

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

Answer: D

NEW QUESTION 840

- (Exam Topic 2)

Which of the following key risk indicators (KRIs) is MOST effective for monitoring risk related to a bring your own device (BYOD) program?

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

Answer: D

NEW QUESTION 841

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 843

- (Exam Topic 2)

Which of the following is MOST commonly compared against the risk appetite?

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

Answer: D

NEW QUESTION 844

- (Exam Topic 2)

Which of the following is MOST important when defining controls?

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

Answer: C

NEW QUESTION 847

- (Exam Topic 2)

Which of the following is a detective control?

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

Answer: B

NEW QUESTION 852

- (Exam Topic 2)

An organization plans to migrate sensitive information to a public cloud infrastructure. Which of the following is the GREATEST security risk in this scenario?

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

Answer: A

NEW QUESTION 857

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 861

- (Exam Topic 2)

An external security audit has reported multiple findings related to control noncompliance. Which of the following would be MOST important for the risk practitioner to communicate to senior management?

- A. A recommendation for internal audit validation
- B. Plans for mitigating the associated risk
- C. Suggestions for improving risk awareness training
- D. The impact to the organization's risk profile

Answer: D

NEW QUESTION 866

- (Exam Topic 2)

After migrating a key financial system to a new provider, it was discovered that a developer could gain access to the production environment. Which of the following is the BEST way to mitigate the risk in this situation?

- A. Escalate the issue to the service provider.
- B. Re-certify the application access controls.
- C. Remove the developer's access.
- D. Review the results of pre-migration testing.

Answer: B

NEW QUESTION 867

- (Exam Topic 2)

Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?

- A. Enhance the security awareness program.
- B. Increase the frequency of incident reporting.
- C. Purchase cyber insurance from a third party.
- D. Conduct a control assessment.

Answer: D

NEW QUESTION 870

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 872

- (Exam Topic 2)

The PRIMARY purpose of a maturity model is to compare the:

- A. current state of key processes to their desired state.
- B. actual KPIs with target KPIs.
- C. organization to industry best practices.
- D. organization to peers.

Answer: A

NEW QUESTION 875

- (Exam Topic 2)

Which of the following is the BEST indication that an organization's risk management program has not reached the desired maturity level?

- A. Significant increases in risk mitigation budgets
- B. Large fluctuations in risk ratings between assessments
- C. A steady increase in the time to recover from incidents

D. A large number of control exceptions

Answer: B

NEW QUESTION 879

- (Exam Topic 2)

Which of the following is the GREATEST risk associated with the use of data analytics?

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

Answer: C

NEW QUESTION 882

- (Exam Topic 2)

Whose risk tolerance matters MOST when making a risk decision?

- A. Customers who would be affected by a breach
- B. Auditors, regulators and standards organizations
- C. The business process owner of the exposed assets
- D. The information security manager

Answer: C

NEW QUESTION 887

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 892

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 895

- (Exam Topic 2)

Which of the following BEST promotes commitment to controls?

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

Answer: A

NEW QUESTION 898

- (Exam Topic 2)

Deviation from a mitigation action plan's completion date should be determined by which of the following?

- A. Change management as determined by a change control board
- B. Benchmarking analysis with similar completed projects
- C. Project governance criteria as determined by the project office
- D. The risk owner as determined by risk management processes

Answer: D

NEW QUESTION 903

- (Exam Topic 2)

A risk practitioner has learned that an effort to implement a risk mitigation action plan has stalled due to lack of funding. The risk practitioner should report that the associated risk has been:

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

Answer: B

NEW QUESTION 905

- (Exam Topic 2)

Which of the following BEST helps to balance the costs and benefits of managing IT risk?

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

Answer: A

NEW QUESTION 906

- (Exam Topic 2)

Which of these documents is MOST important to request from a cloud service provider during a vendor risk assessment?

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

Answer: B

NEW QUESTION 907

- (Exam Topic 2)

Which of the following is the BEST approach for determining whether a risk action plan is effective?

- A. Comparing the remediation cost against budget
- B. Assessing changes in residual risk
- C. Assessing the inherent risk
- D. Monitoring changes of key performance indicators (KPIs)

Answer: B

NEW QUESTION 908

- (Exam Topic 2)

Which of the following is MOST influential when management makes risk response decisions?

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

Answer: A

NEW QUESTION 911

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 913

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 914

.....

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 First Try
- * CRISC Practice Test Questions in Multiple Choice Formats and Updates for 1 Year