

CRISC Dumps

Certified in Risk and Information Systems Control

<https://www.certleader.com/CRISC-dumps.html>



NEW QUESTION 1

- (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 2

- (Exam Topic 3)

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 3

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 4

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 5

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 6

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 7

- (Exam Topic 3)

When of the following provides the MOST tenable evidence that a business process control is effective?

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

Answer: C

NEW QUESTION 8

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 9

- (Exam Topic 3)

Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?

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

Answer: D

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 13

- (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 17

- (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 19

- (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 23

- (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 28

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 30

- (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 35

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 38

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 40

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 43

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 47

- (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 52

- (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 53

- (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 54

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 58

- (Exam Topic 3)

An organization is analyzing the risk of shadow IT usage. Which of the following is the MOST important input into the assessment?

- A. Business benefits of shadow IT
- B. Application-related expresses
- C. Classification of the data
- D. Volume of data

Answer: A

NEW QUESTION 63

- (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 64

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 67

- (Exam Topic 3)

Vulnerabilities have been detected on an organization's systems. Applications installed on these systems will not operate if the underlying servers are updated. Which of the following is the risk practitioner's BEST course of action?

- A. Recommend the business change the application.
- B. Recommend a risk treatment plan.
- C. Include the risk in the next quarterly update to management.
- D. Implement compensating controls.

Answer: D

NEW QUESTION 69

- (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 72

- (Exam Topic 3)

The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:

- A. inconsistencies between security policies and procedures
- B. possible noncompliant activities that lead to data disclosure
- C. leading or lagging key risk indicators (KRIs)
- D. unknown threats to undermine existing access controls

Answer: B

NEW QUESTION 77

- (Exam Topic 3)

Which of the following is MOST important for senior management to review during an acquisition?

- A. Risk appetite and tolerance
- B. Risk framework and methodology
- C. Key risk indicator (KRI) thresholds
- D. Risk communication plan

Answer: A

NEW QUESTION 81

- (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 83

- (Exam Topic 3)

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-party security team
- C. The relationship owner
- D. Legal representation of the business

Answer: C

NEW QUESTION 87

- (Exam Topic 3)

Which of the following should be management's PRIMARY focus when key risk indicators (KRIs) begin to rapidly approach defined thresholds?

- A. Designing compensating controls
- B. Determining if KRIs have been updated recently
- C. Assessing the effectiveness of the incident response plan
- D. Determining what has changed in the environment

Answer: D

NEW QUESTION 92

- (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: A

NEW QUESTION 93

- (Exam Topic 3)

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 95

- (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 98

- (Exam Topic 3)

Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:

- A. a threat.
- B. a vulnerability.
- C. an impact
- D. a control.

Answer: B

NEW QUESTION 103

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 107

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 111

- (Exam Topic 3)

Which of the following is the MOST appropriate action when a tolerance threshold is exceeded?

- A. Communicate potential impact to decision makers.
- B. Research the root cause of similar incidents.
- C. Verify the response plan is adequate.
- D. Increase human resources to respond in the interim.

Answer: A

NEW QUESTION 113

- (Exam Topic 3)

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 118

- (Exam Topic 3)

Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

- A. Key performance indicators (KPIs)
- B. Risk heat maps
- C. Internal audit findings
- D. Periodic penetration testing

Answer: A

NEW QUESTION 121

- (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 125

- (Exam Topic 3)

Which of the following will BEST help to ensure new IT policies address the enterprise's requirements?

- A. involve IT leadership in the policy development process
- B. Require business users to sign acknowledgment of the poises
- C. involve business owners in the pokey development process
- D. Provide policy owners with greater enforcement authority

Answer: B

NEW QUESTION 128

- (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 133

- (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 134

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 136

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 141

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 142

- (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 147

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 150

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 155

- (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 157

- (Exam Topic 3)

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 160

- (Exam Topic 3)

Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

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

Answer: C

NEW QUESTION 162

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 163

- (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 168

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 173

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 177

- (Exam Topic 3)

A risk practitioner has been asked by executives to explain how existing risk treatment plans would affect risk posture at the end of the year. Which of the following is MOST helpful in responding to this request?

- A. Assessing risk with no controls in place
- B. Showing projected residual risk
- C. Providing peer benchmarking results
- D. Assessing risk with current controls in place

Answer: D

NEW QUESTION 181

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 184

- (Exam Topic 3)

Which of the following is the BEST key control indicator (KCI) for risk related to IT infrastructure failure?

- A. Number of times the recovery plan is reviewed
- B. Number of successful recovery plan tests
- C. Percentage of systems with outdated virus protection
- D. Percentage of employees who can work remotely

Answer: B

NEW QUESTION 186

- (Exam Topic 3)

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 188

- (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 192

- (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 193

- (Exam Topic 3)

Who should be responsible (of evaluating the residual risk after a compensating control has been

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

D. Risk practitioner

Answer: D

NEW QUESTION 194

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 199

- (Exam Topic 3)

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 202

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 205

- (Exam Topic 3)

When performing a risk assessment of a new service to support a ewe Business process. which of the following should be done FRST10 ensure continuity of operations?

- A. a identity 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 209

- (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 210

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 213

- (Exam Topic 3)

Winch of the following key control indicators (KCI)s BEST indicates whether security requirements are identified and managed throughout a project He 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: D

NEW QUESTION 215

- (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 220

- (Exam Topic 3)

Which of the following provides the MOST useful information when developing a risk profile for management approval?

- A. Residual risk and risk appetite
- B. Strength of detective and preventative controls
- C. Effectiveness and efficiency of controls
- D. Inherent risk and risk tolerance

Answer: A

NEW QUESTION 221

- (Exam Topic 3)

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

- A. Monitoring
- B. Analysis
- C. Identification
- D. Response selection

Answer: A

NEW QUESTION 226

- (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 229

- (Exam Topic 3)

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

- A. Relevance to the business process
- B. Regulatory compliance requirements
- C. Cost-benefit analysis
- D. Comparison against best practice

Answer: B

NEW QUESTION 230

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 231

- (Exam Topic 3)

Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

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

Answer: A

NEW QUESTION 232

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 235

- (Exam Topic 3)

Which of the following is the MOST effective way to incorporate stakeholder concerns when developing risk scenarios?

- A. Evaluating risk impact
- B. Establishing key performance indicators (KPIs)
- C. Conducting internal audits
- D. Creating quarterly risk reports

Answer: A

NEW QUESTION 240

- (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 242

- (Exam Topic 3)

The GREATEST benefit of including low-probability, high-impact events in a risk assessment is the ability to:

- A. develop a comprehensive risk mitigation strategy
- B. develop understandable and realistic risk scenarios
- C. identify root causes for relevant events
- D. perform an aggregated cost-benefit analysis

Answer: D

NEW QUESTION 247

- (Exam Topic 3)

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 252

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 256

- (Exam Topic 3)

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 261

- (Exam Topic 3)

Which of the following is MOST helpful in preventing risk events from materializing?

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

Answer: A

NEW QUESTION 262

- (Exam Topic 3)

Which of the following is the BEST method of creating risk awareness in an organization?

- A. Marking the risk register available to project stakeholders
- B. Ensuring senior management commitment to risk training
- C. Providing regular communication to risk managers
- D. Appointing the risk manager from the business units

Answer: B

NEW QUESTION 265

- (Exam Topic 3)

Effective risk communication BEST benefits an organization by:

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

Answer: A

NEW QUESTION 268

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 270

- (Exam Topic 3)

Which of the following is the MOST effective control to ensure user access is maintained on a least-privilege basis?

- A. User authorization
- B. User recertification
- C. Change log review
- D. Access log monitoring

Answer: B

NEW QUESTION 274

- (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 278

- (Exam Topic 2)

Which of the following is the PRIMARY role of the board of directors in corporate risk governance?

- A. Approving operational strategies and objectives
- B. Monitoring the results of actions taken to mitigate risk
- C. Ensuring the effectiveness of the risk management program
- D. Ensuring risk scenarios are identified and recorded in the risk register

Answer: C

NEW QUESTION 280

- (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 283

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 286

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 288

- (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 293

- (Exam Topic 2)

Which of the following would MOST likely drive the need to review and update key performance indicators (KPIs) for critical IT assets?

- A. The outsourcing of related IT processes
- B. Outcomes of periodic risk assessments
- C. Changes in service level objectives
- D. Findings from continuous monitoring

Answer: B

NEW QUESTION 298

- (Exam Topic 2)

A recent internal risk review reveals the majority of core IT application recovery time objectives (RTOs) have exceeded the maximum time defined by the business application owners. Which of the following is MOST likely to change as a result?

- A. Risk forecasting
- B. Risk tolerance
- C. Risk likelihood

D. Risk appetite

Answer: B

NEW QUESTION 299

- (Exam Topic 2)

Which of The following is the PRIMARY consideration when establishing an organization's risk management methodology?

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

Answer: A

NEW QUESTION 304

- (Exam Topic 2)

Which of the following is performed after a risk assessment is completed?

- A. Defining risk taxonomy
- B. Identifying vulnerabilities
- C. Conducting an impact analysis
- D. Defining risk response options

Answer: C

NEW QUESTION 308

- (Exam Topic 2)

An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?

- A. Implement IT systems in alignment with business objectives.
- B. Review metrics and key performance indicators (KPIs).
- C. Review design documentation of IT systems.
- D. Evaluate compliance with legal and regulatory requirements.

Answer: D

NEW QUESTION 312

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 315

- (Exam Topic 2)

Risk aggregation in a complex organization will be MOST successful when:

- A. using the same scales in assessing risk
- B. utilizing industry benchmarks
- C. using reliable qualitative data for risk Hems
- D. including primarily low level risk factors

Answer: A

NEW QUESTION 318

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 323

- (Exam Topic 2)

Which of the following would qualify as a key performance indicator (KPI)?

- A. Aggregate risk of the organization
- B. Number of identified system vulnerabilities
- C. Number of exception requests processed in the past 90 days
- D. Number of attacks against the organization's website

Answer: B

NEW QUESTION 325

- (Exam Topic 2)

Which of the following is MOST helpful in verifying that the implementation of a risk mitigation control has been completed as intended?

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

Answer: D

NEW QUESTION 326

- (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 331

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 335

- (Exam Topic 2)

The BEST key performance indicator (KPI) to measure the effectiveness of a vendor risk management program is the percentage of:

- A. vendors providing risk assessments on time.
- B. vendor contracts reviewed in the past year.
- C. vendor risk mitigation action items completed on time.
- D. vendors that have reported control-related incidents.

Answer: A

NEW QUESTION 336

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 337

- (Exam Topic 2)

After identifying new risk events during a project, the project manager's NEXT step should be to:

- A. determine if the scenarios need to be accepted or responded to.
- B. record the scenarios into the risk register.
- C. continue with a qualitative risk analysis.
- D. continue with a quantitative risk analysis.

Answer: B

NEW QUESTION 342

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 346

- (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 351

- (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 356

- (Exam Topic 2)

An organization is planning to outsource its payroll function to an external service provider Which of the following should be the MOST important consideration when selecting the provider?

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

Answer: B

NEW QUESTION 361

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 364

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 368

- (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 370

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 371

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 374

- (Exam Topic 2)

Following a significant change to a business process, a risk practitioner believes the associated risk has been reduced. The risk practitioner should advise the risk owner to FIRST

- A. review the key risk indicators.
- B. conduct a risk analysis.
- C. update the risk register
- D. reallocate risk response resources.

Answer: A

NEW QUESTION 379

- (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 381

- (Exam Topic 2)

Who is accountable for risk treatment?

- A. Enterprise risk management team
- B. Risk mitigation manager
- C. Business process owner
- D. Risk owner

Answer: D

NEW QUESTION 385

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 388

- (Exam Topic 2)

Which of the following should management consider when selecting a risk mitigation option?

- A. Maturity of the enterprise architecture
- B. Cost of control implementation

- C. Reliability of key performance indicators (KPIs)
- D. Reliability of key risk indicators (KPIs)

Answer: B

NEW QUESTION 389

- (Exam Topic 2)

Which of the following is the PRIMARY reason for conducting peer reviews of risk analysis?

- A. To enhance compliance with standards
- B. To minimize subjectivity of assessments
- C. To increase consensus among peers
- D. To provide assessments for benchmarking

Answer: B

NEW QUESTION 393

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 397

- (Exam Topic 2)

A control owner identifies that the organization's shared drive contains personally identifiable information (PII) that can be accessed by all personnel. Which of the following is the MOST effective risk response?

- A. Protect sensitive information with access controls.
- B. Implement a data loss prevention (DLP) solution.
- C. Re-communicate the data protection policy.
- D. Implement a data encryption solution.

Answer: A

NEW QUESTION 400

- (Exam Topic 2)

Which of the following is the PRIMARY reason to establish the root cause of an IT security incident?

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

Answer: D

NEW QUESTION 403

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 404

- (Exam Topic 2)

Which of the following is the PRIMARY benefit of identifying and communicating with stakeholders at the onset of an IT risk assessment?

- A. Obtaining funding support
- B. Defining the risk assessment scope
- C. Selecting the risk assessment framework
- D. Establishing inherent risk

Answer: B

NEW QUESTION 408

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 413

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 414

- (Exam Topic 2)

An organization has outsourced its lease payment process to a service provider who lacks evidence of compliance with a necessary regulatory standard. Which risk treatment was adopted by the organization?

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

Answer: A

NEW QUESTION 417

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 418

- (Exam Topic 2)

Which of the following would MOST likely cause a risk practitioner to reassess risk scenarios?

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

Answer: C

NEW QUESTION 419

- (Exam Topic 2)

To mitigate the risk of using a spreadsheet to analyze financial data, IT has engaged a third-party vendor to deploy a standard application to automate the process. Which of the following parties should own the risk associated with calculation errors?

- A. business owner
- B. IT department
- C. Risk manager
- D. Third-party provider

Answer: A

NEW QUESTION 422

- (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 426

- (Exam Topic 2)

An organization has just implemented changes to close an identified vulnerability that impacted a critical business process. What should be the NEXT course of action?

- A. Redesign the heat map.
- B. Review the risk tolerance.
- C. Perform a business impact analysis (BIA)
- D. Update the risk register.

Answer: D

NEW QUESTION 427

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 428

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 431

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 436

- (Exam Topic 2)

An organization has decided to implement an emerging technology and incorporate the new capabilities into its strategic business plan. Business operations for the technology will be outsourced. What will be the risk practitioner's PRIMARY role during the change?

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

Answer: B

NEW QUESTION 437

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 442

- (Exam Topic 2)

The implementation of a risk treatment plan will exceed the resources originally allocated for the risk response. Which of the following should be the risk owner's NEXT action?

- A. Perform a risk assessment.
- B. Accept the risk of not implementing.
- C. Escalate to senior management.

D. Update the implementation plan.

Answer: C

NEW QUESTION 445

- (Exam Topic 2)

Which of the following would MOST likely result in updates to an IT risk appetite statement?

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

Answer: D

NEW QUESTION 449

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 454

- (Exam Topic 2)

Which of the following MOST effectively limits the impact of a ransomware attack?

- A. Cyber insurance
- B. Cryptocurrency reserve
- C. Data backups
- D. End user training

Answer: C

NEW QUESTION 458

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 463

- (Exam Topic 2)

Which of the following is MOST important for an organization to have in place when developing a risk management framework?

- A. A strategic approach to risk including an established risk appetite
- B. A risk-based internal audit plan for the organization
- C. A control function within the risk management team
- D. An organization-wide risk awareness training program

Answer: A

NEW QUESTION 468

- (Exam Topic 2)

Which of the following BEST facilitates the development of effective IT risk scenarios?

- A. Utilization of a cross-functional team
- B. Participation by IT subject matter experts
- C. Integration of contingency planning
- D. Validation by senior management

Answer: A

NEW QUESTION 470

- (Exam Topic 2)

A payroll manager discovers that fields in certain payroll reports have been modified without authorization. Which of the following control weaknesses could have contributed MOST to this problem?

- A. The user requirements were not documented.
- B. Payroll files were not under the control of a librarian.
- C. The programmer had access to the production programs.
- D. The programmer did not involve the user in testing.

Answer: B

NEW QUESTION 471

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 474

- (Exam Topic 2)

The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

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

Answer: C

NEW QUESTION 475

- (Exam Topic 2)

Which of the following BEST measures the efficiency of an incident response process?

- A. Number of incidents escalated to management
- B. Average time between changes and updating of escalation matrix
- C. Average gap between actual and agreed response times
- D. Number of incidents lacking responses

Answer: C

NEW QUESTION 477

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 479

- (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 482

- (Exam Topic 2)

What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium	Low	Low
Tango	Medium	Low	Medium
Uniform	High	High	High
Victor	High	Medium	Medium

- A. Relative positions on the risk map
- B. Risk treatment options

- C. Capability of enterprise to implement
- D. The multiple risk factors addressed by a chosen response

Answer: A

NEW QUESTION 486

- (Exam Topic 1)

An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?

- A. Invoke the disaster recovery plan during an incident.
- B. Prepare a cost-benefit analysis of alternatives available
- C. Implement redundant infrastructure for the application.
- D. Reduce the recovery time by strengthening the response team.

Answer: C

NEW QUESTION 487

- (Exam Topic 3)

Which of the following is the GREATEST benefit for an organization with a strong risk awareness culture?

- A. Reducing the involvement by senior management
- B. Using more risk specialists
- C. Reducing the need for risk policies and guidelines
- D. Discussing and managing risk as a team

Answer: D

NEW QUESTION 491

- (Exam Topic 3)

Which of the following should be the GREATEST concern for an organization that uses open source software applications?

- A. Lack of organizational policy regarding open source software
- B. Lack of reliability associated with the use of open source software
- C. Lack of monitoring over installation of open source software in the organization
- D. Lack of professional support for open source software

Answer: A

NEW QUESTION 492

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 493

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 497

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 499

- (Exam Topic 3)

An IT department has provided a shared drive for personnel to store information to which all employees have access. Which of the following parties is accountable for the risk of potential loss of confidential information?

- A. Risk manager
- B. Data owner
- C. End user
- D. IT department

Answer: D

NEW QUESTION 503

- (Exam Topic 3)

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 506

- (Exam Topic 3)

Which of the following would be a risk practitioner's BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

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

Answer: A

NEW QUESTION 507

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 512

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 517

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 518

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 521

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 525

- (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 526

- (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 529

- (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 531

- (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 535

- (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 538

- (Exam Topic 3)

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

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

D. Maintaining a risk register

Answer: A

NEW QUESTION 543

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 544

- (Exam Topic 3)

When developing risk treatment alternatives for a Business case, it is MOST helpful to show risk reduction based on:

- A. cost-benefit analysis.
- B. risk appetite.
- C. regulatory guidelines
- D. control efficiency

Answer: A

NEW QUESTION 547

- (Exam Topic 3)

Which of the following is the BEST approach to mitigate the risk associated with a control deficiency?

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

Answer: C

NEW QUESTION 552

- (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 557

- (Exam Topic 2)

Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?

- A. Trends in IT resource usage
- B. Trends in IT maintenance costs
- C. Increased resource availability
- D. Increased number of incidents

Answer: A

NEW QUESTION 560

- (Exam Topic 2)

A control owner responsible for the access management process has developed a machine learning model to automatically identify excessive access privileges. What is the risk practitioner's BEST course of action?

- A. Review the design of the machine learning model against control objectives.
- B. Adopt the machine learning model as a replacement for current manual access reviews.
- C. Ensure the model assists in meeting regulatory requirements for access controls.
- D. Discourage the use of emerging technologies in key processes.

Answer: A

NEW QUESTION 565

- (Exam Topic 2)

Which of the following is the BEST indicator of the effectiveness of a control action plan's implementation?

- A. Increased number of controls
- B. Reduced risk level
- C. Increased risk appetite
- D. Stakeholder commitment

Answer: B

NEW QUESTION 569

- (Exam Topic 2)

What is the MOST important consideration when aligning IT risk management with the enterprise risk management (ERM) framework?

- A. Risk and control ownership
- B. Senior management participation
- C. Business unit support
- D. Risk nomenclature and taxonomy

Answer: B

NEW QUESTION 573

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 578

- (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 582

- (Exam Topic 2)

Which of the following would be of GREATEST assistance when justifying investment in risk response strategies?

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

Answer: C

NEW QUESTION 586

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 589

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 591

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 592

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 593

- (Exam Topic 2)

Which of the following is MOST likely to be impacted as a result of a new policy which allows staff members to remotely connect to the organization's IT systems via personal or public computers?

- A. Risk appetite
- B. Inherent risk
- C. Key risk indicator (KRI)
- D. Risk tolerance

Answer: B

NEW QUESTION 594

- (Exam Topic 2)

A risk owner should be the person accountable for:

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

Answer: C

NEW QUESTION 599

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 603

- (Exam Topic 2)

An organization has implemented a system capable of comprehensive employee monitoring. Which of the following should direct how the system is used?

- A. Organizational strategy
- B. Employee code of conduct
- C. Industry best practices
- D. Organizational policy

Answer: D

NEW QUESTION 606

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 608

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 610

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 611

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 614

- (Exam Topic 1)

A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application. Who should have the authority to accept the associated risk?

- A. Business continuity director
- B. Disaster recovery manager
- C. Business application owner
- D. Data center manager

Answer: C

NEW QUESTION 617

- (Exam Topic 1)

From a business perspective, which of the following is the MOST important objective of a disaster recovery test?

- A. The organization gains assurance it can recover from a disaster
- B. Errors are discovered in the disaster recovery process.
- C. All business critical systems are successfully tested.
- D. All critical data is recovered within recovery time objectives (RTOs).

Answer: B

NEW QUESTION 618

- (Exam Topic 1)

A review of an organization s controls has determined its data loss prevention {DLP} system is currently failing to detect outgoing emails containing credit card data. Which of the following would be MOST impacted?

- A. Key risk indicators (KRIs)
- B. Inherent risk
- C. Residual risk
- D. Risk appetite

Answer: C

NEW QUESTION 619

- (Exam Topic 1)

Which of the following is the MAIN reason to continuously monitor IT-related risk?

- A. To redefine the risk appetite and risk tolerance levels based on changes in risk factors

- B. To update the risk register to reflect changes in levels of identified and new IT-related risk
- C. To ensure risk levels are within acceptable limits of the organization's risk appetite and risk tolerance
- D. To help identify root causes of incidents and recommend suitable long-term solutions

Answer: C

NEW QUESTION 624

- (Exam Topic 1)

Which of the following changes would be reflected in an organization's risk profile after the failure of a critical patch implementation?

- A. Risk tolerance is decreased.
- B. Residual risk is increased.
- C. Inherent risk is increased.
- D. Risk appetite is decreased

Answer: D

NEW QUESTION 625

- (Exam Topic 1)

Which of the following will BEST mitigate the risk associated with IT and business misalignment?

- A. Establishing business key performance indicators (KPIs)
- B. Introducing an established framework for IT architecture
- C. Establishing key risk indicators (KRIs)
- D. Involving the business process owner in IT strategy

Answer: D

NEW QUESTION 629

- (Exam Topic 1)

The MOST important characteristic of an organization's policies is to reflect the organization's:

- A. risk assessment methodology.
- B. risk appetite.
- C. capabilities
- D. asset value.

Answer: B

NEW QUESTION 630

- (Exam Topic 1)

Which of the following is MOST helpful in identifying new risk exposures due to changes in the business environment?

- A. Standard operating procedures
- B. SWOT analysis
- C. Industry benchmarking
- D. Control gap analysis

Answer: B

NEW QUESTION 635

- (Exam Topic 1)

Who is the MOST appropriate owner for newly identified IT risk?

- A. The manager responsible for IT operations that will support the risk mitigation efforts
- B. The individual with authority to commit organizational resources to mitigate the risk
- C. A project manager capable of prioritizing the risk remediation efforts
- D. The individual with the most IT risk-related subject matter knowledge

Answer: B

NEW QUESTION 636

- (Exam Topic 1)

A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:

- A. identification.
- B. treatment.
- C. communication.
- D. assessment

Answer: C

NEW QUESTION 640

- (Exam Topic 1)

Which of the following would be considered a vulnerability?

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

Answer: A

NEW QUESTION 645

- (Exam Topic 1)

Which of the following is the MOST cost-effective way to test a business continuity plan?

- A. Conduct interviews with key stakeholders.
- B. Conduct a tabletop exercise.
- C. Conduct a disaster recovery exercise.
- D. Conduct a full functional exercise.

Answer: B

NEW QUESTION 646

- (Exam Topic 1)

Which of the following would be the BEST way to help ensure the effectiveness of a data loss prevention (DLP) control that has been implemented to prevent the loss of credit card data?

- A. Testing the transmission of credit card numbers
- B. Reviewing logs for unauthorized data transfers
- C. Configuring the DLP control to block credit card numbers
- D. Testing the DLP rule change control process

Answer: A

NEW QUESTION 647

- (Exam Topic 1)

A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

- A. Document the finding in the risk register.
- B. Invoke the incident response plan.
- C. Re-evaluate key risk indicators.
- D. Modify the design of the control.

Answer: A

NEW QUESTION 648

- (Exam Topic 1)

IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would be MOST helpful?

- A. IT risk register
- B. List of key risk indicators
- C. Internal audit reports
- D. List of approved projects

Answer: A

NEW QUESTION 649

- (Exam Topic 1)

Which of the following activities would BEST contribute to promoting an organization-wide risk-aware culture?

- A. Performing a benchmark analysis and evaluating gaps
- B. Conducting risk assessments and implementing controls
- C. Communicating components of risk and their acceptable levels
- D. Participating in peer reviews and implementing best practices

Answer: C

NEW QUESTION 653

- (Exam Topic 1)

Which of the following is the MOST important consideration when developing an organization's risk taxonomy?

- A. Leading industry frameworks
- B. Business context
- C. Regulatory requirements
- D. IT strategy

Answer: B

NEW QUESTION 655

- (Exam Topic 1)

Which of the following helps ensure compliance with a nonrepudiation policy requirement for electronic transactions?

- A. Digital signatures
- B. Encrypted passwords
- C. One-time passwords
- D. Digital certificates

Answer: A

NEW QUESTION 659

- (Exam Topic 1)

Which of the following is the MOST important requirement for monitoring key risk indicators (KRIs) using log analysis?

- A. Obtaining logs in an easily readable format
- B. Providing accurate logs in a timely manner
- C. Collecting logs from the entire set of IT systems
- D. implementing an automated log analysis tool

Answer: B

NEW QUESTION 661

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 665

- (Exam Topic 1)

Which of the following is the PRIMARY reason for a risk practitioner to use global standards related to risk management?

- A. To build an organizational risk-aware culture
- B. To continuously improve risk management processes
- C. To comply with legal and regulatory requirements
- D. To identify gaps in risk management practices

Answer: B

NEW QUESTION 666

- (Exam Topic 1)

A risk practitioner is organizing risk awareness training for senior management. Which of the following is the MOST important topic to cover in the training session?

- A. The organization's strategic risk management projects
- B. Senior management roles and responsibilities
- C. The organization's risk appetite and tolerance
- D. Senior management allocation of risk management resources

Answer: B

NEW QUESTION 669

- (Exam Topic 1)

Which of the following aspects of an IT risk and control self-assessment would be MOST important to include in a report to senior management?

- A. Changes in control design
- B. A decrease in the number of key controls
- C. Changes in control ownership
- D. An increase in residual risk

Answer: D

NEW QUESTION 671

- (Exam Topic 1)

Which of the following is the MOST important outcome of reviewing the risk management process?

- A. Assuring the risk profile supports the IT objectives
- B. Improving the competencies of employees who performed the review
- C. Determining what changes should be made to IS policies to reduce risk
- D. Determining that procedures used in risk assessment are appropriate

Answer: A

NEW QUESTION 676

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 677

- (Exam Topic 1)

Which of the following is the FIRST step in managing the risk associated with the leakage of confidential data?

- A. Maintain and review the classified data inventory.
- B. Implement mandatory encryption on data
- C. Conduct an awareness program for data owners and users.
- D. Define and implement a data classification policy

Answer: D

NEW QUESTION 679

- (Exam Topic 1)

Which of the following would be MOST useful when measuring the progress of a risk response action plan?

- A. Percentage of mitigated risk scenarios
- B. Annual loss expectancy (ALE) changes
- C. Resource expenditure against budget
- D. An up-to-date risk register

Answer: D

NEW QUESTION 681

- (Exam Topic 1)

A trusted third party service provider has determined that the risk of a client's systems being hacked is low. Which of the following would be the client's BEST course of action?

- A. Perform their own risk assessment
- B. Implement additional controls to address the risk.
- C. Accept the risk based on the third party's risk assessment
- D. Perform an independent audit of the third party.

Answer: C

NEW QUESTION 686

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 691

- (Exam Topic 1)

During an IT risk scenario review session, business executives question why they have been assigned ownership of IT-related risk scenarios. They feel IT risk is technical in nature and therefore should be owned by IT. Which of the following is the BEST way for the risk practitioner to address these concerns?

- A. Describe IT risk scenarios in terms of business risk.
- B. Recommend the formation of an executive risk council to oversee IT risk.
- C. Provide an estimate of IT system downtime if IT risk materializes.
- D. Educate business executives on IT risk concepts.

Answer: A

NEW QUESTION 693

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 697

- (Exam Topic 1)

Which of the following is the BEST method for assessing control effectiveness?

- A. Ad hoc control reporting
- B. Control self-assessment
- C. Continuous monitoring
- D. Predictive analytics

Answer: C

NEW QUESTION 701

- (Exam Topic 1)

A data processing center operates in a jurisdiction where new regulations have significantly increased penalties for data breaches. Which of the following elements of the risk register is MOST important to update to reflect this change?

- A. Risk impact
- B. Risk trend
- C. Risk appetite
- D. Risk likelihood

Answer: A

NEW QUESTION 704

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 706

- (Exam Topic 1)

An effective control environment is BEST indicated by controls that:

- A. minimize senior management's risk tolerance.
- B. manage risk within the organization's risk appetite.
- C. reduce the thresholds of key risk indicators (KRIs).
- D. are cost-effective to implement

Answer: B

NEW QUESTION 710

- (Exam Topic 1)

During testing, a risk practitioner finds the IT department's recovery time objective (RTO) for a key system does not align with the enterprise's business continuity plan (BCP). Which of the following should be done NEXT?

- A. Report the gap to senior management
- B. Consult with the IT department to update the RTO
- C. Complete a risk exception form.
- D. Consult with the business owner to update the BCP

Answer: A

NEW QUESTION 712

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 715

- (Exam Topic 1)

A rule-based data loss prevention (DLP) tool has recently been implemented to reduce the risk of sensitive data leakage. Which of the following is MOST likely to change as a result of this implementation?

- A. Risk likelihood
- B. Risk velocity
- C. Risk appetite
- D. Risk impact

Answer: A

NEW QUESTION 720

- (Exam Topic 1)

Risk mitigation procedures should include:

- A. buying an insurance policy.
- B. acceptance of exposures
- C. deployment of counter measures.
- D. enterprise architecture implementation.

Answer: B

NEW QUESTION 721

- (Exam Topic 1)

Which of the following will BEST quantify the risk associated with malicious users in an organization?

- A. Business impact analysis
- B. Risk analysis
- C. Threat risk assessment
- D. Vulnerability assessment

Answer: A

NEW QUESTION 725

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CRISC Exam with Our Prep Materials Via below:

<https://www.certleader.com/CRISC-dumps.html>