# Isaca

## Exam Questions CRISC

Certified in Risk and Information Systems Control

# About Exambible

***Your Partner of IT Exam***

# Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

# Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**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)
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 4**
- (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 5**
- (Exam Topic 4)
Which of the following is the MOST important consideration for effectively maintaining a risk register?

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

**Answer:** B

**NEW QUESTION 6**
- (Exam Topic 4)
A risk practitioner has collaborated with subject matter experts from the IT department to develop a large list of potential key risk indicators (KRIs) for all IT operations within the organization of the following, who should review the completed list and select the appropriate KRIs for implementation?

A. IT security managers
B. IT control owners
C. IT auditors
D. IT risk owners

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

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

**Answer:** B

**NEW QUESTION 9**
- (Exam Topic 4)
During a risk assessment, a key external technology supplier refuses to provide control design and effectiveness information, citing confidentiality concerns. What should the risk practitioner do NEXT?

A. Escalate the non-cooperation to management
B. Exclude applicable controls from the assessment.
C. Review the supplier's contractual obligations.
D. Request risk acceptance from the business process owner.

**Answer:** C

**NEW QUESTION 10**
- (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 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 14**
- (Exam Topic 4)
Which of the following is the MOST important information to cover a business continuity awareness Ira nine, 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 15**
- (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 16**

- (Exam Topic 4)
Which of the following key performance indicators (KPis) would BEST measure me risk of a service outage when using a Software as a Service (SaaS) vendors

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

**Answer:** C

**NEW QUESTION 20**
- (Exam Topic 4)
An organization has recently hired a large number of part-time employees. During the annual audit, it was discovered that many user IDs and passwords were documented in procedure manuals for use by the part-time employees. Which of the following BEST describes this situation?

A. Threat
B. Risk
C. Vulnerability
D. Policy violation

**Answer:** B

**NEW QUESTION 24**
- (Exam Topic 4)
Which of the following is the GREATEST benefit of using IT risk scenarios?

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

**Answer:** C

**NEW QUESTION 26**
- (Exam Topic 4)
An organization has decided to implement a new Internet of Things (loT) solution. Which of the following should be done FIRST when addressing security concerns associated with this new technology?

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

**Answer:** A

**NEW QUESTION 30**
- (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 34**
- (Exam Topic 4)
A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

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

**Answer:** B

**NEW QUESTION 38**
- (Exam Topic 4)
After undertaking a risk assessment of a production system, the MOST appropriate action is fcr 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 42**
- (Exam Topic 4)
If preventive controls cannot be Implemented due to technology limitations, which of the following should be done FIRST to reduce risk7

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 43**
- (Exam Topic 4)
An organization has decided to commit to a business activity with the knowledge that the risk exposure is higher than the risk appetite. Which of the following is the risk practitioner's MOST important action related to this decision?

A. Recommend risk remediation
B. Change the level of risk appetite
C. Document formal acceptance of the risk
D. Reject the business initiative

**Answer:** C

**NEW QUESTION 45**
- (Exam Topic 4)
An organization uses one centralized single sign-on (SSO) control to cover many applications. Which of the following is the BEST course of action when a new application is added to the environment after testing of the SSO control has been completed?

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

**Answer:** A

**NEW QUESTION 49**
- (Exam Topic 4)
Which of the following is the PRIMARY reason for a risk practitioner to review an organization's IT asset inventory?

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

**Answer:** C

**NEW QUESTION 50**
- (Exam Topic 4)
An organization is participating in an industry benchmarking study that involves providing customer transaction records for analysis Which of the following is the MOST important control to ensure the privacy of customer information?

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

**Answer:** C

**NEW QUESTION 54**
- (Exam Topic 4)
What is senior management's role in the RACI model when tasked with reviewing monthly status reports provided by risk owners?

A. Accountable
B. Informed
C. Responsible
D. Consulted

**Answer:** B

**NEW QUESTION 56**
- (Exam Topic 4)
In order to determining a risk is under-controlled the risk practitioner will need to

A. understand the risk tolerance
B. monitor and evaluate IT performance
C. identify risk management best practices

D. determine the sufficiency of the IT risk budget

**Answer:** A

**NEW QUESTION 57**
- (Exam Topic 4)
Which of the following is the MOST effective way to help ensure accountability for managing risk?

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

**Answer:** A

**NEW QUESTION 59**
- (Exam Topic 4)
When is the BEST to identify risk associated with major project to determine a mitigation plan?

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

**Answer:** D

**NEW QUESTION 63**
- (Exam Topic 4)
A recent regulatory requirement has the potential to affect an organization's use of a third party to supply outsourced business services. Which of the following is the BEST course of action?

A. Conduct a gap analysis.
B. Terminate the outsourcing agreement.
C. Identify compensating controls.
D. Transfer risk to the third party.

**Answer:** A

**NEW QUESTION 66**
- (Exam Topic 4)
Which of the following is the PRIMARY purpose of creating and documenting control procedures?

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

**Answer:** D

**NEW QUESTION 67**
- (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 identity all relevant issues.
B. be too costly
C. violate laws in other countries
D. be too line consuming

**Answer:** C

**NEW QUESTION 69**
- (Exam Topic 4)
Which of the following provides the BEST assurance of the effectiveness of vendor security controls?

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

**Answer:** C

**NEW QUESTION 71**
- (Exam Topic 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 75**
- (Exam Topic 4)
Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?

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

**Answer:** D

**NEW QUESTION 77**
- (Exam Topic 4)
Which of the following would MOST likely cause management to unknowingly accept excessive risk?

A. Satisfactory audit results
B. Risk tolerance being set too low
C. Inaccurate risk ratings
D. Lack of preventive controls

**Answer:** C

**NEW QUESTION 82**
- (Exam Topic 4)
An organization has allowed several employees to retire early in order to avoid layoffs Many of these employees have been subject matter experts for critical assets Which type of risk is MOST likely to materialize?

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

**Answer:** B

**NEW QUESTION 85**
- (Exam Topic 4)
A penetration test reveals several vulnerabilities in a web-facing application. Which of the following should be the FIRST step in selecting a risk response?

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

**Answer:** C

**NEW QUESTION 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 94**
- (Exam Topic 4)
Which of the following BEST enables risk-based decision making in support of a business continuity plan (BCP)?

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

**Answer:** A

**NEW QUESTION 96**

- (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 100**
- (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 fallowing 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 101**
- (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 104**
- (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 109**
- (Exam Topic 3)
Which of the following is MOST important to include in a risk assessment of an emerging technology?

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

**Answer:** D

**NEW QUESTION 111**
- (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 114**
- (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 118**
- (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 122**
- (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 124**
- (Exam Topic 3)
Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?

A. Evaluating the impact to control objectives
B. Conducting a root cause analysis
C. Validating the adequacy of current processes
D. Reconfiguring the IT infrastructure

**Answer:** B

**NEW QUESTION 128**
- (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 131**
- (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 136**
- (Exam Topic 3)
Which of the following should be an element of the risk appetite of an organization?

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

**Answer:** B

**NEW QUESTION 138**
- (Exam Topic 3)
Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?

A. Percentage of high-risk vulnerabilities missed
B. Number of high-risk vulnerabilities outstanding

C. Defined thresholds for high-risk vulnerabilities
D. Percentage of high-risk vulnerabilities addressed

**Answer:** D

**NEW QUESTION 139**
- (Exam Topic 3)
Several network user accounts were recently created without the required management approvals. Which of the following would be the risk practitioner's BEST recommendation to address this situation?

A. Conduct a comprehensive compliance review.
B. Develop incident response procedures for noncompliance.
C. Investigate the root cause of noncompliance.
D. Declare a security breach and Inform management.

**Answer:** C

**NEW QUESTION 140**
- (Exam Topic 3)
Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

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

**Answer:** B

**NEW QUESTION 144**
- (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 149**
- (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 150**
- (Exam Topic 3)
Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

A. Automated access revocation
B. Daily transaction reconciliation
C. Rule-based data analytics
D. Role-based user access model

**Answer:** B

**NEW QUESTION 155**
- (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 159**
- (Exam Topic 3)

Which of the following is the PRIMARY risk management responsibility of the second line of defense?

A. Monitoring risk responses
B. Applying risk treatments
C. Providing assurance of control effectiveness
D. Implementing internal controls

**Answer:** A

**NEW QUESTION 163**
- (Exam Topic 3)
Which of the following is MOST important when developing key risk indicators (KRIs)?

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

**Answer:** C

**NEW QUESTION 166**
- (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 169**
- (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 172**
- (Exam Topic 3)
An organization has been notified that a disgruntled, terminated IT administrator has tried to break into the corporate network. Which of the following discoveries should be of GREATEST concern to the organization?

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

**Answer:** A

**NEW QUESTION 177**
- (Exam Topic 3)
While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

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

**Answer:** B

**NEW QUESTION 181**
- (Exam Topic 3)
When of the following is the MOST significant exposure when an application uses individual user accounts to access the underlying database?

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

**Answer:** C

**NEW QUESTION 182**
- (Exam Topic 3)
Senior management has asked the risk practitioner for the overall residual risk level for a process that contains numerous risk scenarios. Which of the following should be provided?

A. The sum of residual risk levels for each scenario
B. The loss expectancy for aggregated risk scenarios
C. The highest loss expectancy among the risk scenarios
D. The average of anticipated residual risk levels

**Answer:** D

**NEW QUESTION 183**
- (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 187**
- (Exam Topic 3)
Who should have the authority to approve an exception to a control?

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

**Answer:** C

**NEW QUESTION 189**
- (Exam Topic 3)
An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?

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

**Answer:** B

**NEW QUESTION 194**
- (Exam Topic 3)
Which of the following BEST indicates how well a web infrastructure protects critical information from an attacker?

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

**Answer:** D

**NEW QUESTION 198**
- (Exam Topic 3)
Which of the following is the PRIMARY role of a data custodian in the risk management process?

A. Performing periodic data reviews according to policy
B. Reporting and escalating data breaches to senior management
C. Being accountable for control design
D. Ensuring data is protected according to the classification

**Answer:** D

**NEW QUESTION 199**
- (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 203**
- (Exam Topic 3)
Which of the following scenarios represents a threat?

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

**Answer:** D

**NEW QUESTION 205**
- (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 207**
- (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 211**
- (Exam Topic 3)
Which of the following provides the MOST useful information when determining if a specific control should be implemented?

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

**Answer:** B

**NEW QUESTION 213**
- (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 214**
- (Exam Topic 3)
Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

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

**Answer:** B

**NEW QUESTION 219**
- (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 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)
The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

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

**Answer:** C

**NEW QUESTION 227**
- (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 231**
- (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 severs receiving automata patches
C. Number of unremediated vulnerabilities
D. Number of intrusion attempts

**Answer:** D

**NEW QUESTION 233**
- (Exam Topic 3)
Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?

A. Segregation of duties
B. Three lines of defense
C. Compliance review
D. Quality assurance review

**Answer:** B

**NEW QUESTION 236**
- (Exam Topic 3)
While reviewing the risk register, a risk practitioner notices that different business units have significant variances in inherent risk for the same risk scenario. Which of the following is the BEST course of action?

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

**Answer:** B

**NEW QUESTION 240**
- (Exam Topic 3)
Which of the following provides the MOST useful information to determine risk exposure following control implementations?

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

**Answer:** C

**NEW QUESTION 241**
- (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 243**
- (Exam Topic 3)
The risk associated with an asset after controls are applied can be expressed as:

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

**Answer:** C

**NEW QUESTION 248**
- (Exam Topic 3)
Winch of the following key control indicators (KCIs) 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:** A

**NEW QUESTION 250**
- (Exam Topic 3)
Which of the following is the BEST reason to use qualitative measures to express residual risk levels related to emerging threats?

A. Qualitative measures require less ongoing monitoring.
B. Qualitative measures are better aligned to regulatory requirements.
C. Qualitative measures are better able to incorporate expert judgment.
D. Qualitative measures are easier to update.

**Answer:** C

**NEW QUESTION 251**
- (Exam Topic 3)
Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

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

**Answer:** B

**NEW QUESTION 256**
- (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 261**

- (Exam Topic 3)
Which of the following is the MOST important consideration for protecting data assets m a Business application system?

A. Application controls are aligned with data classification lutes
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 265**
- (Exam Topic 3)
Legal and regulatory risk associated with business conducted over the Internet is driven by:

A. the jurisdiction in which an organization has its principal headquarters
B. international law and a uniform set of regulations.
C. the laws and regulations of each individual country
D. international standard-setting bodies.

**Answer:** C

**NEW QUESTION 268**
- (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 272**
- (Exam Topic 3)
When evaluating enterprise IT risk management it is MOST important to:

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

**Answer:** B

**NEW QUESTION 277**
- (Exam Topic 3)
Which of the following is MOST important to the integrity of a security log?

A. Least privilege access
B. Inability to edit
C. Ability to overwrite
D. Encryption

**Answer:** B

**NEW QUESTION 281**
- (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 285**
- (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 290**
- (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 292**
- (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 295**
- (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 296**
- (Exam Topic 3)
What are the MOST essential attributes of an effective Key control indicator (KCI)?

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

**Answer:** B

**NEW QUESTION 300**
- (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 304**
- (Exam Topic 3)
In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

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

**Answer:** B

**NEW QUESTION 309**
- (Exam Topic 3)
When updating the risk register after a risk assessment, which of the following is MOST important to include?

A. Historical losses due to past risk events
B. Cost to reduce the impact and likelihood
C. Likelihood and impact of the risk scenario
D. Actor and threat type of the risk scenario

**Answer:** C

**NEW QUESTION 310**
- (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 315**
- (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 317**
- (Exam Topic 3)
Which of the following is MOST important to the successful development of IT risk scenarios?

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

**Answer:** C

**NEW QUESTION 319**
- (Exam Topic 3)
Which of the following would be MOST useful to senior management when determining an appropriate risk response?

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

**Answer:** A

**NEW QUESTION 320**
- (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 323**
- (Exam Topic 3)
Analyzing trends in key control indicators (KCIs) BEST enables a risk practitioner to proactively identify impacts on an organization's:

A. risk classification methods
B. risk-based capital allocation
C. risk portfolio
D. risk culture

**Answer:** C

**NEW QUESTION 325**
- (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 328**
- (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 332**
- (Exam Topic 3)
Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

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

**Answer:** B

**NEW QUESTION 334**
- (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 338**
- (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 339**
- (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 341**
- (Exam Topic 3)
Which of the following is the BEST way to quantify the likelihood of risk materialization?

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

**Answer:** D

**NEW QUESTION 344**
- (Exam Topic 3)
A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

A. Single sign-on
B. Audit trail review
C. Multi-factor authentication
D. Data encryption at rest

**Answer:** B

**NEW QUESTION 347**
- (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 351**
- (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 354**
- (Exam Topic 3)
An organization learns of a new ransomware attack affecting organizations worldwide. Which of the following should be done FIRST to reduce the likelihood of infection from the attack?

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

**Answer:** A

**NEW QUESTION 358**
- (Exam Topic 3)
To help identify high-risk situations, an organization should:

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

**Answer:** A

**NEW QUESTION 362**
- (Exam Topic 3)
Which of We 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 prowler 10 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 363**
- (Exam Topic 3)
A highly regulated organization acquired a medical technology startup company that processes sensitive personal information with weak data protection controls. Which of the following is the BEST way for the
acquiring company to reduce its risk while still enabling the flexibility needed by the startup company?

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

**Answer:** A

**NEW QUESTION 364**
- (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 369**
- (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 370**
- (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 373**
- (Exam Topic 3)
An organization is implementing internet of Things (loT) technology to control temperature and lighting in its headquarters. Which of the following should be of GREATEST concern?

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

**Answer:** D

**NEW QUESTION 377**
- (Exam Topic 4)
Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?

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

**Answer:** A

**NEW QUESTION 380**
- (Exam Topic 4)
Which of the following is MOST important to ensure when reviewing an organization's risk register?

A. Risk ownership is recorded.
B. Vulnerabilities have separate entries.
C. Control ownership is recorded.
D. Residual risk is less than inherent risk.

**Answer:** A

**NEW QUESTION 385**
- (Exam Topic 4)
Which of the following is the MOST important objective from a cost perspective for considering aggregated risk responses in an organization?

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

**Answer:** C

**NEW QUESTION 388**
- (Exam Topic 4)
Recovery the objectives (RTOs) should be based on

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

**Answer:** C

**NEW QUESTION 392**
- (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 393**
- (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 394**
- (Exam Topic 4)
Which of the following is the MOST comprehensive resource for prioritizing the implementation of information systems controls?

A. Data classification policy
B. Emerging technology trends
C. The IT strategic plan
D. The risk register

**Answer:** C

**NEW QUESTION 399**
- (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 404**
- (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 -partf3ecurity team
C. The relationship owner
D. Legal representation of the business

**Answer:** C

**NEW QUESTION 409**
- (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 412**
- (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 413**
- (Exam Topic 4)
Which of the following BEST enables senior management lo compare the ratings of risk scenarios?

A. Key risk indicators (KRIs)
B. Key performance indicators (KPIs)
C. Control self-assessment (CSA)
D. Risk heat map

**Answer:** D

**NEW QUESTION 418**
- (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 421**
- (Exam Topic 4)
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 sell-assessment (CSA)
D. Build a provision for risk

**Answer:** C

**NEW QUESTION 426**
- (Exam Topic 4)
Who should be responsible (of evaluating the residual risk after a compensating control has been

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

**Answer:** D

**NEW QUESTION 430**
- (Exam Topic 4)
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 432**
- (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 435**
- (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 439**
- (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 443**
- (Exam Topic 4)
Which of the following is MOST important for mitigating ethical risk when establishing accountability for control ownership?

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

**Answer:** B

**NEW QUESTION 446**
- (Exam Topic 4)
Which of the following provides the MOST comprehensive information when developing a risk profile for a system?

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

**Answer:** B

**NEW QUESTION 450**
- (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 455**
- (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 457**

- (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 462**
- (Exam Topic 4)
Which of the following is the PRIMARY reason for sharing risk assessment reports with senior stakeholders?

A. To support decision-making for risk response
B. To hold risk owners accountable for risk action plans
C. To secure resourcing for risk treatment efforts
D. To enable senior management to compile a risk profile

**Answer:** A

**NEW QUESTION 467**
- (Exam Topic 4)
Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

A. Verifying that project objectives are met
B. Identifying project cost overruns
C. Leveraging an independent review team
D. Reviewing the project initiation risk matrix

**Answer:** A

**NEW QUESTION 469**
- (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 472**
- (Exam Topic 4)
The PRIMARY objective of collecting information and reviewing documentation when performing periodic risk analysis should be to:

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

**Answer:** D

**NEW QUESTION 473**
- (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 478**
- (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 481**
- (Exam Topic 4)
Which of the following is the MOST effective way 10 identify an application backdoor prior to implementation'?

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

**Answer:** B

**NEW QUESTION 483**
- (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 488**
- (Exam Topic 4)
The BEST indicator of the risk appetite of an organization is the

A. regulatory environment of the organization
B. risk management capability of the organization
C. board of directors' response to identified risk factors
D. importance assigned to IT in meeting strategic goals

**Answer:** B

**NEW QUESTION 492**
- (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 496**
- (Exam Topic 4)
Which of the following is the PRIMARY objective of risk management?

A. Identify and analyze risk.
B. Achieve business objectives
C. Minimi2e business disruptions.
D. Identify threats and vulnerabilities.

**Answer:** B

**NEW QUESTION 498**
- (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 503**
- (Exam Topic 4)
Which of the following should be used as the PRIMARY basis for evaluating the state of an organization's cloud computing environment against leading practices?

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

**Answer:** A

**NEW QUESTION 505**
- (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 506**
- (Exam Topic 4)
Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

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

**Answer:** A

**NEW QUESTION 509**
- (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 514**
- (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 515**
- (Exam Topic 4)
Which of the following would BEST mitigate an identified risk scenario?

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

**Answer:** C

**NEW QUESTION 518**
- (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 519**
- (Exam Topic 4)
A global organization has implemented an application that does not address all privacy requirements across multiple jurisdictions. Which of the following risk responses has the organization adopted with regard to privacy requirements?

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

**Answer:** A

**NEW QUESTION 523**
- (Exam Topic 4)
Which of the following observations from a third-party service provider review would be of GREATEST concern to a risk practitioner?

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

**Answer:** C

**NEW QUESTION 525**
- (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 529**
- (Exam Topic 4)
Which of the following is a risk practitioner's MOST important responsibility in managing risk acceptance that exceeds risk tolerance?

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

**Answer:** A

**NEW QUESTION 531**
- (Exam Topic 4)
Which of the blowing is MOST important when implementing an organization s security policy?

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

**Answer:** A

**NEW QUESTION 534**
- (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 536**
- (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 537**
- (Exam Topic 4)
An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

A. Identify the regulatory bodies that may highlight this gap

B. Highlight news articles about data breaches
C. Evaluate the risk as a measure of probable loss
D. Verify if competitors comply with a similar policy

**Answer:** B

**NEW QUESTION 542**
- (Exam Topic 4)
Which of the following is the PRIMARY reason to engage business unit managers in risk management processes'?

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

**Answer:** C

**NEW QUESTION 547**
- (Exam Topic 4)
Which of the following BEST facilitates the identification of appropriate key performance indicators (KPIs) for a risk management program?

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

**Answer:** C

**NEW QUESTION 549**
- (Exam Topic 4)
When defining thresholds for control key performance indicators (KPIs). it is MOST helpful to align:

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

**Answer:** B

**NEW QUESTION 551**
- (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 554**
- (Exam Topic 4)
Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

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

**Answer:** A

**NEW QUESTION 556**
- (Exam Topic 4)
A risk practitioner observed Vial a high number of pokey exceptions were approved by senior management. Which of the following is the risk practitioner’s BEST course of action to determine root cause?

A. Review the risk profile
B. Review pokey change history
C. interview the control owner
D. Perform control testing

**Answer:** C

**NEW QUESTION 560**

- (Exam Topic 4)
When reviewing the business continuity plan (BCP) of an online sales order system, a risk practitioner notices that the recovery time objective (RTO) has a shorter lime than what is defined in the disaster recovery plan (DRP). Which of the following is the BEST way for the risk practitioner to address this concern?

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

**Answer:** D

**NEW QUESTION 565**
- (Exam Topic 4)
An organization has experienced a cyber attack that exposed customer personally identifiable information (Pll) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

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

**Answer:** C

**NEW QUESTION 568**
- (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 573**
- (Exam Topic 4)
Which of the following is the BEST way to help ensure risk will be managed properly after a business process has been re-engineered?

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

**Answer:** A

**NEW QUESTION 577**
- (Exam Topic 4)
An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?

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

**Answer:** C

**NEW QUESTION 581**
- (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 582**
- (Exam Topic 4)
Which of the following is MOST important to promoting a risk-aware culture?

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

**Answer:** D

**NEW QUESTION 587**
- (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 592**
- (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 596**
- (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 599**
- (Exam Topic 4)
Which of the following will BEST help to ensure implementation of corrective action plans?

A. Establishing employee awareness training
B. Assigning accountability to risk owners
C. Selling target dates to complete actions
D. Contracting to third parties

**Answer:** B

**NEW QUESTION 600**
- (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 602**
- (Exam Topic 4)
When creating a separate IT risk register for a large organization, which of the following is MOST important to consider with regard to the existing corporate risk 'register?

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

**Answer:** D

**NEW QUESTION 603**
- (Exam Topic 4)
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 607**
- (Exam Topic 4)
Which of the following would be the BEST way for a risk practitioner to validate the effectiveness of a patching program?

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

**Answer:** C

**NEW QUESTION 611**
- (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 612**
- (Exam Topic 4)
Which of the following is a risk practitioner's BEST recommendation upon learning that an employee inadvertently disclosed sensitive data to a vendor?

A. Enroll the employee in additional security training.
B. Invoke the incident response plan.
C. Conduct an internal audit.
D. Instruct the vendor to delete the data.

**Answer:** B

**NEW QUESTION 617**
- (Exam Topic 4)
An organization is adopting blockchain for a new financial system. Which of the following should be the GREATEST concern for a risk practitioner evaluating the system's production readiness?

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

**Answer:** A

**NEW QUESTION 618**
- (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 623**
- (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 627**
- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 628**
- (Exam Topic 4)
Which of the following is the result of a realized risk scenario?

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

**Answer:** D

**NEW QUESTION 632**
- (Exam Topic 4)
Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?

A. Internal auditor
B. Asset owner
C. Finance manager
D. Control owner

**Answer:** B

**NEW QUESTION 633**
- (Exam Topic 4)
Which of the following is MOST important to update when an organization's risk appetite changes?

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

**Answer:** A

**NEW QUESTION 634**
- (Exam Topic 4)
After an annual risk assessment is completed, which of the following would be MOST important to communicate to stakeholders?

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

**Answer:** B

**NEW QUESTION 639**
- (Exam Topic 4)
An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:

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

**Answer:** D

**NEW QUESTION 644**
- (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 648**
- (Exam Topic 4)
Which of the following is the GREATEST benefit of identifying appropriate risk owners?

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

**Answer:** A

**NEW QUESTION 651**
- (Exam Topic 4)
Which of the following is the ULTIMATE goal of conducting a privacy impact analysis (PIA)?

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

**Answer:** A

**NEW QUESTION 653**
- (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 657**
- (Exam Topic 4)
When evaluating a number of potential controls for treating risk, it is MOST important to consider:

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

**Answer:** C

**NEW QUESTION 662**
- (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 663**
- (Exam Topic 4)
Which organization is implementing a project to automate the purchasing process, including the modification of approval controls. Which of the following tasks is lie responsibility of the risk practitioner*?

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

**Answer:** B

**NEW QUESTION 667**
- (Exam Topic 4)
An organization is implementing robotic process automation (RPA) to streamline business processes. Given that implementation of this technology is expected to impact existing controls, which of the following is the risk practitioner's BEST course of action?

A. Reassess whether mitigating controls address the known risk in the processes.
B. Update processes to address the new technology.
C. Update the data governance policy to address the new technology.
D. Perform a gap analysis of the impacted processes.

**Answer:** A

**NEW QUESTION 671**
- (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 673**
- (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 677**
- (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 682**
- (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 687**
- (Exam Topic 4)
An organization recently implemented a machine learning-based solution to monitor IT usage and analyze user behavior in an effort to detect internal fraud. Which of the following is MOST likely to be reassessed as a result of this initiative?

A. Risk likelihood
B. Risk culture
C. Risk appetite
D. Risk capacity

**Answer:** A

**NEW QUESTION 688**
- (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 692**
- (Exam Topic 4)
Which of the following will BEST ensure that controls adequately support business goals and objectives?

A. Using the risk management process
B. Enforcing strict disciplinary procedures in case of noncompliance
C. Reviewing results of the annual company external audit
D. Adopting internationally accepted controls

**Answer:** A

**NEW QUESTION 693**
- (Exam Topic 4)
Which of the following should be the PRIMARY basis for prioritizing risk responses?

A. The impact of the risk
B. The replacement cost of the business asset
C. The cost of risk mitigation controls
D. The classification of the business asset

**Answer:** A

**NEW QUESTION 696**
- (Exam Topic 4)
A newly incorporated enterprise needs to secure its information assets From a governance perspective which of the following should be done FIRST?

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

**Answer:** D

**NEW QUESTION 699**
- (Exam Topic 4)
An internal audit report reveals that a legacy system is no longer supported Which of the following is the risk practitioner's MOST important action before recommending a risk response'

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

**Answer:** B

**NEW QUESTION 704**
- (Exam Topic 4)
Which of the following is MOST important when determining risk appetite?

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

**Answer:** C

**NEW QUESTION 708**
- (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 713**
- (Exam Topic 4)
Which of the following is MOST important for an organization to consider when developing its IT strategy?

A. IT goals and objectives
B. Organizational goals and objectives
C. The organization's risk appetite statement
D. Legal and regulatory requirements

**Answer:** C

**NEW QUESTION 717**

- (Exam Topic 4)
it was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern1?

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

**Answer:** C

**NEW QUESTION 720**
- (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 722**
- (Exam Topic 3)
Which of the following is the BEST way to manage the risk associated with malicious activities performed by database administrators (DBAs)?

A. Activity logging and monitoring
B. Periodic access review
C. Two-factor authentication
D. Awareness training and background checks

**Answer:** A

**NEW QUESTION 726**
- (Exam Topic 3)
Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

A. Senior management has approved the control design.
B. Inherent risk has been reduced from original levels.
C. Residual risk remains within acceptable levels.
D. Costs for control maintenance are reasonable.

**Answer:** C

**NEW QUESTION 730**
- (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 734**
- (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 736**
- (Exam Topic 3)
A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual
risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

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

**Answer:** D

**NEW QUESTION 740**
- (Exam Topic 3)
To minimize the risk of a potential acquisition being exposed externally, an organization has selected a few key employees to be engaged in the due diligence process. A member of the due diligence team realizes a close acquaintance is a high-ranking IT professional at a subsidiary of the company about to be acquired. What is the BEST course of action for this team member?

A. Enforce segregation of duties.
B. Disclose potential conflicts of interest.
C. Delegate responsibilities involving the acquaintance.
D. Notify the subsidiary's legal team.

**Answer:** B

**NEW QUESTION 743**
- (Exam Topic 3)
Which of the following would be MOST helpful to an information security management team when allocating resources to mitigate exposures?

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

**Answer:** C

**NEW QUESTION 744**
- (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 745**
- (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 750**
- (Exam Topic 3)
An information system for a key business operation is being moved from an in-house application to a Software as a Service (SaaS) vendor. Which of the following will have the GREATEST impact on the ability to monitor risk?

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

**Answer:** A

**NEW QUESTION 753**
- (Exam Topic 3)
Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

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

**Answer:** A

**NEW QUESTION 754**
- (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 756**
- (Exam Topic 3)
Which of the following BEST indicates that additional or improved controls ate needed m 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 758**
- (Exam Topic 3)
What is the PRIMARY purpose of a business impact analysis (BIA)?

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

**Answer:** D

**NEW QUESTION 760**
- (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 761**
- (Exam Topic 3)
Which of the following practices BEST mitigates risk related to enterprise-wide ethical decision making in a multi-national organization?

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

**Answer:** A

**NEW QUESTION 766**
- (Exam Topic 3)
An organization must make a choice among multiple options to respond to a risk. The stakeholders cannot agree and decide to postpone the decision. Which of the following risk responses has the organization adopted?

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

**Answer:** D

**NEW QUESTION 770**
- (Exam Topic 3)
An organization's risk register contains a large volume of risk scenarios that senior management considers overwhelming. Which of the following would BEST help to improve the risk register?

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

**Answer:** D

**NEW QUESTION 775**
- (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 776**
- (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 778**
- (Exam Topic 3)
Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

**Answer:** A

**NEW QUESTION 779**
- (Exam Topic 3)
After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?

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

**Answer:** B

**NEW QUESTION 782**
- (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 786**
- (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 791**
- (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 796**

- (Exam Topic 3)
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

A. Ensure compliance.
B. Identify trends.
C. Promote a risk-aware culture.
D. Optimize resources needed for controls

**Answer:** A

**NEW QUESTION 797**
- (Exam Topic 3)
Which of the following poses the GREATEST risk to an organization's operations during a major it transformation?

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

**Answer:** D

**NEW QUESTION 800**
- (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 804**
- (Exam Topic 3)
Which of the following is the BEST way to assess the effectiveness of an access management process?

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

**Answer:** B

**NEW QUESTION 808**
- (Exam Topic 3)
Which of the following BEST mitigates the risk of sensitive personal data leakage from a software development environment?

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

**Answer:** C

**NEW QUESTION 811**
- (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 816**
- (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 821**
- (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 822**
- (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 827**
- (Exam Topic 3)
Which of the following approaches would BEST help to identify relevant risk scenarios?

A. Engage line management in risk assessment workshops.
B. Escalate the situation to risk leadership.
C. Engage internal audit for risk assessment workshops.
D. Review system and process documentation.

**Answer:** A

**NEW QUESTION 828**
- (Exam Topic 3)
Which of the following is the MOST common concern associated with outsourcing to a service provider?

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

**Answer:** C

**NEW QUESTION 831**
- (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 834**
- (Exam Topic 3)
Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?

A. Unknown vulnerabilities
B. Legacy technology systems
C. Network isolation
D. Overlapping threats

**Answer:** D

**NEW QUESTION 838**
- (Exam Topic 3)
Which of me 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 840**
- (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 843**
- (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 847**
- (Exam Topic 3)
Which of the following would be a risk practitioner'$ BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

A. Manage cyber risk according to the organization's risk management framework.
B. Define cyber roles and responsibilities across the organization
C. Conduct cyber risk awareness training tailored specifically for senior management
D. Implement a cyber risk program based on industry best practices

**Answer:** B

**NEW QUESTION 848**
- (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 defected over a period of time
C. Number of alerts generated by the anti-virus software
D. Frequency of anti-vinjs software updates

**Answer:** A

**NEW QUESTION 852**
- (Exam Topic 3)
An organization is implementing encryption for data at rest to reduce the risk associated with unauthorized access. Which of the following MUST be considered to assess the residual risk?

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

**Answer:** D

**NEW QUESTION 856**
- (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 857**
- (Exam Topic 3)
An organization practices the principle of least privilege. To ensure access remains appropriate, application owners should be required to review user access rights on a regular basis by obtaining:

A. business purpose documentation and software license counts
B. an access control matrix and approval from the user's manager
C. documentation indicating the intended users of the application
D. security logs to determine the cause of invalid login attempts

**Answer:** B

**NEW QUESTION 859**
- (Exam Topic 3)
Which of the following MUST be updated to maintain an IT risk register?

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

**Answer:** C

**NEW QUESTION 862**
- (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 866**
- (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 870**
- (Exam Topic 3)
Accountability for a particular risk is BEST represented in a:

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

**Answer:** D

**NEW QUESTION 871**
- (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 876**
- (Exam Topic 3)
While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

A. review and update the policies to align with industry standards.
B. determine that the policies should be updated annually.
C. report that the policies are adequate and do not need to be updated frequently.
D. review the policies against current needs to determine adequacy.

**Answer:** D

**NEW QUESTION 877**
- (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 881**
- (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 (Al) solutions into the organization?

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

**Answer:** B

**NEW QUESTION 884**
- (Exam Topic 3)
Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?

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

**Answer:** D

**NEW QUESTION 889**
- (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 892**
- (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 895**
- (Exam Topic 2)
Which of the following risk scenarios would be the GREATEST concern as a result of a single sign-on implementation?

A. User access may be restricted by additional security.
B. Unauthorized access may be gained to multiple systems.
C. Security administration may become more complex.
D. User privilege changes may not be recorded.

**Answer:** B

**NEW QUESTION 899**
- (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 902**
- (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 904**
- (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 906**
- (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 911**
- (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 916**
- (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 921**
.....

# Relate Links

**100% Pass Your CRISC Exam with Exambible Prep Materials**

https://www.exambible.com/CRISC-exam/

# Contact us

**We are proud of our high-quality customer service, which serves you around the clock 24/7.**

**Viste -** https://www.exambible.com/