



**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)

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

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

**Answer: C**

#### NEW QUESTION 4

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 5

- (Exam Topic 4)

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 6

- (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 7

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 8

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 9

- (Exam Topic 4)

A poster has been displayed in a data center that reads, "Anyone caught taking photographs in the data center may be subject to disciplinary action." Which of the following control types has been implemented?

- A. Corrective
- B. Detective
- C. Deterrent
- D. Preventative

**Answer: A**

#### NEW QUESTION 10

- (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 10

- (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 13

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 14

- (Exam Topic 4)

Which of the following roles should be assigned accountability for monitoring risk levels?

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

**Answer: C**

#### NEW QUESTION 19

- (Exam Topic 4)

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

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

**Answer: D**

#### NEW QUESTION 23

- (Exam Topic 4)

Which of the following provides the MOST useful information for developing key risk indicators (KRIs)?

- A. Business impact analysis (BIA) results
- B. Risk scenario ownership
- C. Risk thresholds
- D. Possible causes of materialized risk

**Answer: C**

#### NEW QUESTION 28

- (Exam Topic 4)

An organization's control environment is MOST effective when:

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

**Answer: A**

#### NEW QUESTION 31

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 32

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 35

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 39

- (Exam Topic 4)

Which of the following should be the FIRST consideration when establishing a new risk governance program?

- A. Developing an ongoing awareness and training program
- B. Creating policies and standards that are easy to comprehend
- C. Embedding risk management into the organization
- D. Completing annual risk assessments on critical resources

**Answer: B**

**NEW QUESTION 43**

- (Exam Topic 4)

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

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

**Answer: A**

**NEW QUESTION 47**

- (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 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)

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

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

**Answer: C**

**NEW QUESTION 59**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 64**

- (Exam Topic 4)

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 65**

- (Exam Topic 4)

Which of the following is the BEST method to maintain a common view of IT risk within an organization?

- A. Collecting data for IT risk assessment
- B. Establishing and communicating the IT risk profile
- C. Utilizing a balanced scorecard
- D. Performing and publishing an IT risk analysis

**Answer:** C

**NEW QUESTION 67**

- (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 69**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 72**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 75**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 77**

- (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 81**

- (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 85

- (Exam Topic 4)

A legacy application used for a critical business function relies on software that has reached the end of extended support. Which of the following is the MOST effective control to manage this application?

- A. Subscribe to threat intelligence to monitor external attacks.
- B. Apply patches for a newer version of the application.
- C. Segment the application within the existing network.
- D. Increase the frequency of regular system and data backups.

**Answer:** D

#### NEW QUESTION 89

- (Exam Topic 4)

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

- A. Risk control assessment
- B. Audit reports with risk ratings
- C. Penetration test results
- D. Business impact analysis (BIA)

**Answer:** D

#### NEW QUESTION 90

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 94

- (Exam Topic 3)

Which of the following is the BEST way to determine the potential organizational impact of emerging privacy regulations?

- A. Evaluate the security architecture maturity.
- B. Map the new requirements to the existing control framework.
- C. Charter a privacy steering committee.
- D. Conduct a privacy impact assessment (PIA).

**Answer:** D

#### NEW QUESTION 97

- (Exam Topic 3)

Which of the following is MOST useful when communicating risk to management?

- A. Risk policy
- B. Audit report
- C. Risk map
- D. Maturity model

**Answer:** C

#### NEW QUESTION 101

- (Exam Topic 3)

The MAIN reason for creating and maintaining a risk register is to:

- A. assess effectiveness of different projects.
- B. define the risk assessment methodology.
- C. ensure assets have low residual risk.
- D. account for identified key risk factors.

**Answer:** D

#### NEW QUESTION 106



- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 111

- (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 113

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 116

- (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 117

- (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 122

- (Exam Topic 3)

A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

- A. Regulatory requirements may differ in each country.
- B. Data sampling may be impacted by various industry restrictions.
- C. Business advertising will need to be tailored by country.
- D. The data analysis may be ineffective in achieving objectives.

**Answer: A**

#### NEW QUESTION 126

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 131

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 135

- (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 140

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 144

- (Exam Topic 3)

Which of the following is the MOST important consideration when implementing ethical remote work monitoring?

- A. Monitoring is only conducted between official hours of business
- B. Employees are informed of how they are being monitored
- C. Reporting on nonproductive employees is sent to management on a scheduled basis
- D. Multiple data monitoring sources are integrated into security incident response procedures

**Answer: B**

#### NEW QUESTION 145

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 148

- (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 149

- (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 152**

- (Exam Topic 3)

Which of the following is the GREATEST benefit of analyzing logs collected from different systems?

- A. A record of incidents is maintained.
- B. Forensic investigations are facilitated.
- C. Security violations can be identified.
- D. Developing threats are detected earlier.

**Answer: C**

**NEW QUESTION 153**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 158**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 160**

- (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 165**

- (Exam Topic 3)

Which of the following is the BEST recommendation to senior management when the results of a risk and control assessment indicate a risk scenario can only be partially mitigated?

- A. Implement controls to bring the risk to a level within appetite and accept the residual risk.
- B. Implement a key performance indicator (KPI) to monitor the existing control performance.
- C. Accept the residual risk in its entirety and obtain executive management approval.
- D. Separate the risk into multiple components and avoid the risk components that cannot be mitigated.

**Answer: C**

**NEW QUESTION 169**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 170**

- (Exam Topic 3)

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

- A. Corporate risk appetite is communicated to staff members.
- B. Risk owners understand and accept accountability for risk.

- C. Risk policy has been published and acknowledged by employees.
- D. Management encourages the reporting of policy breaches.

**Answer: B**

#### **NEW QUESTION 171**

- (Exam Topic 3)

Which of the following represents a vulnerability?

- A. An identity thief seeking to acquire personal financial data from an organization
- B. Media recognition of an organization's market leadership in its industry
- C. A standard procedure for applying software patches two weeks after release
- D. An employee recently fired for insubordination

**Answer: C**

#### **NEW QUESTION 172**

- (Exam Topic 3)

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

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

**Answer: C**

#### **NEW QUESTION 175**

- (Exam Topic 3)

Which of the following statements BEST illustrates the relationship between key performance indicators (KPIs) and key control indicators (KCIs)?

- A. KPIs measure manual controls, while KCIs measure automated controls.
- B. KPIs and KCIs both contribute to understanding of control effectiveness.
- C. A robust KCI program will replace the need to measure KPIs.
- D. KCIs are applied at the operational level while KPIs are at the strategic level.

**Answer: B**

#### **NEW QUESTION 180**

- (Exam Topic 3)

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

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

**Answer: C**

#### **NEW QUESTION 183**

- (Exam Topic 3)

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

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

**Answer: B**

#### **NEW QUESTION 185**

- (Exam Topic 3)

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

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

**Answer: D**

#### **NEW QUESTION 189**

- (Exam Topic 3)

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

- A. Gap analysis
- B. Risk assessment
- C. Heat map
- D. Risk register

**Answer: C**

#### NEW QUESTION 193

- (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 197

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 199

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 201

- (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 203

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 205

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 207

- (Exam Topic 3)

When of the following 15 MOST important when developing a business case for a proposed security investment?

- A. identification of control requirements
- B. Alignment to business objectives
- C. Consideration of new business strategies
- D. inclusion of strategy for regulatory compliance

**Answer: B**

#### NEW QUESTION 212

- (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 216

- (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 219

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 222

- (Exam Topic 3)

Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?

- A. Ensuring that database changes are correctly applied
- B. Enforcing that changes are authorized
- C. Deterring illicit actions of database administrators
- D. Preventing system developers from accessing production data

**Answer: C**

#### NEW QUESTION 227

- (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 232

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 233**

- (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 238**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 239**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 243**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 248**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 252**

- (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 253**

- (Exam Topic 3)

An organization recently received an independent security audit report of its cloud service provider that indicates significant control weaknesses. What should be done NEXT in response to this report?

- A. Migrate all data to another compliant service provider.
- B. Analyze the impact of the provider's control weaknesses to the business.

- C. Conduct a follow-up audit to verify the provider's control weaknesses.
- D. Review the contract to determine if penalties should be levied against the provider.

**Answer:** B

#### **NEW QUESTION 254**

- (Exam Topic 3)

An organization outsources the processing of us payroll data. A risk practitioner identifies a control weakness at the third party that exposes the payroll data. Who should own this risk?

- A. The third party's IT operations manager
- B. The organization's process owner
- C. The third party's chief risk officer (CRO)
- D. The organization's risk practitioner

**Answer:** B

#### **NEW QUESTION 258**

- (Exam Topic 3)

Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?

- A. Ongoing availability of data
- B. Ability to aggregate data
- C. Ability to predict trends
- D. Availability of automated reporting systems

**Answer:** D

#### **NEW QUESTION 263**

- (Exam Topic 3)

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

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

**Answer:** B

#### **NEW QUESTION 268**

- (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 273**

- (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 277**

- (Exam Topic 3)

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

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

**Answer:** D

#### **NEW QUESTION 280**

- (Exam Topic 3)



The PRIMARY objective of a risk identification process is to:

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

**Answer: B**

#### NEW QUESTION 281

- (Exam Topic 3)

What is the PRIMARY benefit of risk monitoring?

- A. It reduces the number of audit findings.
- B. It provides statistical evidence of control efficiency.
- C. It facilitates risk-aware decision making.
- D. It facilitates communication of threat levels.

**Answer: C**

#### NEW QUESTION 283

- (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 286

- (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 290

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 293

- (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 295

- (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 296

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 297

- (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 302

- (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 306

- (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 307

- (Exam Topic 3)

In which of the following system development life cycle (SDLC) phases should controls be incorporated into system specifications?

- A. Implementation
- B. Development
- C. Design
- D. Feasibility

**Answer: C**

#### NEW QUESTION 310

- (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 311

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 316

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 318

- (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 319

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 321

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 325

- (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 326

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 329

- (Exam Topic 3)

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

- A. Perform a gap analysis.
- B. Prioritize impact to the business units.
- C. Perform a risk assessment.

D. Review the risk tolerance and appetite.

**Answer: C**

**NEW QUESTION 334**

- (Exam Topic 3)

In an organization where each division manages risk independently, which of the following would BEST enable management of risk at the enterprise level?

- A. A standardized risk taxonomy
- B. A list of control deficiencies
- C. An enterprise risk ownership policy
- D. An updated risk tolerance metric

**Answer: A**

**NEW QUESTION 338**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 343**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 348**

- (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 353**

- (Exam Topic 4)

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

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

**Answer: A**

**NEW QUESTION 356**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 361**

- (Exam Topic 4)

A risk practitioner recently discovered that personal information from the production environment is required for testing purposes in non-production environments.

Which of the following is the BEST recommendation to address this situation?

- A. Enable data encryption in the test environment.
- B. Prevent the use of production data in the test environment
- C. De-identify data before being transferred to the test environment.
- D. Enforce multi-factor authentication within the test environment.

**Answer: C**

#### **NEW QUESTION 362**

- (Exam Topic 4)

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

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

**Answer: B**

#### **NEW QUESTION 365**

- (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 369**

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

**Answer: C**

#### **NEW QUESTION 372**

- (Exam Topic 4)

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

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

**Answer: C**

#### **NEW QUESTION 377**

- (Exam Topic 4)

Which of the following BEST enables senior management to 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 378**

- (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 380**

- (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 384**

- (Exam Topic 4)

Which of the following is the MAIN benefit to an organization using key risk indicators (KRIs)?

- A. KRIs assist in the preparation of the organization's risk profile.
- 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 provide an early warning that a risk threshold is about to be reached.

**Answer: D**

**NEW QUESTION 389**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 394**

- (Exam Topic 4)

Which of the following activities BEST facilitates effective risk management throughout the organization?

- A. Reviewing risk-related process documentation
- B. Conducting periodic risk assessments
- C. Performing a business impact analysis (BIA)
- D. Performing frequent audits

**Answer: B**

**NEW QUESTION 395**

- (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 396**

- (Exam Topic 4)

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

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

**Answer: D**

**NEW QUESTION 398**

- (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 399**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 400**

- (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 403**

- (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 408**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 409**

- (Exam Topic 4)

A zero-day vulnerability has been discovered in a globally used brand of hardware server that allows hackers to gain access to affected IT systems. Which of the following is MOST likely to change as a result of this situation?

- A. Control effectiveness
- B. Risk appetite
- C. Risk likelihood
- D. Key risk indicator (KRI)

**Answer: C**

**NEW QUESTION 413**

- (Exam Topic 4)

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

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

**Answer: A**

**NEW QUESTION 417**

- (Exam Topic 4)

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

- A. Technical event

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

**Answer: D**

**NEW QUESTION 418**

- (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 421**

- (Exam Topic 4)

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

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

**Answer: C**

**NEW QUESTION 422**

- (Exam Topic 4)

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

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

**Answer: B**

**NEW QUESTION 423**

- (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 424**

- (Exam Topic 4)

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

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

**Answer: A**

**NEW QUESTION 425**

- (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 429**

- (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 430

- (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 435

- (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 437

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 440

- (Exam Topic 4)

When developing risk scenario using a list of generic scenarios based on industry best practices, it is MOST important 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 441

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 442

- (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 444

- (Exam Topic 4)

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

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

**Answer: C**

#### NEW QUESTION 449

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 451

- (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 456

- (Exam Topic 4)

An organization has experienced a cyber attack that exposed customer personally identifiable information (PII) and caused extended outages of network services. Which of the following stakeholders are MOST important to include in the cyber response team to determine response actions?

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

**Answer: C**

#### NEW QUESTION 460

- (Exam Topic 4)

Which of the following is the GREATEST benefit of centralizing IT systems?

- A. Risk reporting
- B. Risk classification
- C. Risk monitoring
- D. Risk identification

**Answer: C**

#### NEW QUESTION 465

- (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 467

- (Exam Topic 4)

Which of the following should be of GREATEST concern when reviewing the results of an independent control assessment to determine the effectiveness of a vendor's control environment?

- A. The report was provided directly from the vendor.
- B. The risk associated with multiple control gaps was accepted.
- C. The control owners disagreed with the auditor's recommendations.
- D. The controls had recurring noncompliance.

**Answer:** A

**NEW QUESTION 471**

- (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 476**

- (Exam Topic 4)

An organization is considering the adoption of an aggressive business strategy to achieve desired growth. From a risk management perspective, what should the risk practitioner do NEXT?

- A. Identify new threats resorting from the new business strategy
- B. Update risk awareness training to reflect current levels of risk appetite and tolerance
- C. Inform the board of potential risk scenarios associated with aggressive business strategies
- D. Increase the scale for measuring impact due to threat materialization

**Answer:** A

**NEW QUESTION 480**

- (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 482**

- (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 483**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 487**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 488**

- (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 489**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 490**

- (Exam Topic 4)

Which of the following provides the MOST reliable evidence of a control's effectiveness?

- A. A risk and control self-assessment
- B. Senior management's attestation
- C. A system-generated testing report
- D. detailed process walk-through

**Answer:** D

**NEW QUESTION 492**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 493**

- (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 497**

- (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 500**

- (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 505**

- (Exam Topic 4)

Which key performance efficiency (KPI) BEST measures the effectiveness of an organization's disaster recovery program?

- A. Number of service level agreement (SLA) violations
- B. Percentage of recovery issues identified during the exercise
- C. Number of total systems recovered within the recovery point objective (RPO)
- D. Percentage of critical systems recovered within the recovery time objective (RTO)

**Answer: D**

#### NEW QUESTION 506

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 510

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 512

- (Exam Topic 4)

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

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

**Answer: B**

#### NEW QUESTION 513

- (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 514

- (Exam Topic 4)

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

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

**Answer: A**

#### NEW QUESTION 517

- (Exam Topic 4)

After the implementation of Internet 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 of IoT devices
- B. To add new controls to mitigate the risk
- C. To recommend changes to the IoT policy
- D. To confirm the impact to the risk profile

**Answer: D**

#### NEW QUESTION 522

- (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 the 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 527

- (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 532

- (Exam Topic 4)

The MAIN purpose of selecting a risk response is to.

- A. ensure compliance with local regulatory requirements
- B. demonstrate the effectiveness of risk management practices.
- C. ensure organizational awareness of the risk level
- D. mitigate the residual risk to be within tolerance

**Answer: C**

#### NEW QUESTION 536

- (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 540

- (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 545

- (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 547

- (Exam Topic 4)

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

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

**Answer:**

C

**NEW QUESTION 548**

- (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 550**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 552**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 557**

- (Exam Topic 3)

Which of the following BEST indicates that an organization has implemented IT performance requirements?

- A. Service level agreements (SLA)
- B. Vendor references
- C. Benchmarking data
- D. Accountability matrix

**Answer: A**

**NEW QUESTION 560**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 565**

- (Exam Topic 3)

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

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

**Answer: D**

**NEW QUESTION 569**

- (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 573**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 575**

- (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 580**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 584**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 588**

- (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 591**

- (Exam Topic 3)

Which of the following is the STRONGEST indication an organization has ethics management issues?

- A. Employees do not report IT risk issues for fear of consequences.
- B. Internal IT auditors report to the chief information security officer (CISO).
- C. Employees face sanctions for not signing the organization's acceptable use policy.
- D. The organization has only two lines of defense.

**Answer:** A

**NEW QUESTION 593**

- (Exam Topic 3)

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



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

**Answer:** A

**NEW QUESTION 595**

- (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 597**

- (Exam Topic 3)

Which of the following is the FIRST step in risk assessment?

- A. Review risk governance
- B. Asset identification
- C. Identify risk factors
- D. Inherent risk identification

**Answer:** B

**NEW QUESTION 600**

- (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 601**

- (Exam Topic 3)

Which of the following is the BEST course of action to help reduce the probability of an incident recurring?

- A. Perform a risk assessment.
- B. Perform root cause analysis.
- C. Initiate disciplinary action.
- D. Update the incident response plan.

**Answer:** B

**NEW QUESTION 603**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 607**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 612**

- (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 614

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 619

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 624

- (Exam Topic 3)

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

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

**Answer: D**

#### NEW QUESTION 626

- (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 630

- (Exam Topic 3)

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

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

**Answer: A**

#### NEW QUESTION 634

- (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 636

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 641

- (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 646

- (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 648

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 649

- (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 653

- (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 654

- (Exam Topic 3)

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

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

**Answer:**

D

**NEW QUESTION 659**

- (Exam Topic 3)

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

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

**Answer: A**

**NEW QUESTION 663**

- (Exam Topic 3)

Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?

- A. Complete an offsite business continuity exercise.
- B. Conduct a compliance check against standards.
- C. Perform a vulnerability assessment.
- D. Measure the change in inherent risk.

**Answer: C**

**NEW QUESTION 668**

- (Exam Topic 3)

An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

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

**Answer: B**

**NEW QUESTION 673**

- (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 674**

- (Exam Topic 3)

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

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

**Answer: B**

**NEW QUESTION 679**

- (Exam Topic 3)

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

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

**Answer: C**

**NEW QUESTION 682**

- (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 683**

- (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 684**

- (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 688**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 691**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 694**

- (Exam Topic 2)

Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?

- A. Defining expectations in the enterprise risk policy
- B. Increasing organizational resources to mitigate risks
- C. Communicating external audit results
- D. Avoiding risks that could materialize into substantial losses

**Answer:** A

**NEW QUESTION 696**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 701**

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 704

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 706

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 708

- (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 712

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 714

- (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 717

- (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 719

- (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 724

- (Exam Topic 2)

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

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

**Answer: D**

#### NEW QUESTION 725

- (Exam Topic 2)

Which of the following is MOST important when defining controls?

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

**Answer: C**

#### NEW QUESTION 726

- (Exam Topic 2)

Who is accountable for risk treatment?

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

**Answer: D**

#### NEW QUESTION 730

- (Exam Topic 2)

When reporting risk assessment results to senior management, which of the following is MOST important to include to enable risk-based decision making?

- A. Risk action plans and associated owners
- B. Recent audit and self-assessment results
- C. Potential losses compared to treatment cost
- D. A list of assets exposed to the highest risk

**Answer: A**

#### NEW QUESTION 733

- (Exam Topic 2)

Which of the following is a detective control?

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

**Answer: B**

#### NEW QUESTION 734

- (Exam Topic 2)

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

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

**Answer: D**

**NEW QUESTION 737**

- (Exam Topic 2)

When assessing the maturity level of an organization's risk management framework, which of the following deficiencies should be of GREATEST concern to a risk practitioner?

- A. Unclear organizational risk appetite
- B. Lack of senior management participation
- C. Use of highly customized control frameworks
- D. Reliance on qualitative analysis methods

**Answer: C**

**NEW QUESTION 740**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 744**

- (Exam Topic 2)

Who should be responsible for strategic decisions on risk management?

- A. Chief information officer (CIO)
- B. Executive management team
- C. Audit committee
- D. Business process owner

**Answer: B**

**NEW QUESTION 746**

- (Exam Topic 2)

The BEST way to test the operational effectiveness of a data backup procedure is to:

- A. conduct an audit of files stored offsite.
- B. interview employees to compare actual with expected procedures.
- C. inspect a selection of audit trails and backup logs.
- D. demonstrate a successful recovery from backup files.

**Answer: D**

**NEW QUESTION 751**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 754**

- (Exam Topic 2)

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

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

**Answer: D**

**NEW QUESTION 759**

- (Exam Topic 2)

Which of the following resources is MOST helpful when creating a manageable set of IT risk scenarios?

- A. Results of current and past risk assessments
- B. Organizational strategy and objectives



- C. Lessons learned from materialized risk scenarios
- D. Internal and external audit findings

**Answer: B**

**NEW QUESTION 760**

- (Exam Topic 2)

Which of the following conditions presents the GREATEST risk to an application?

- A. Application controls are manual.
- B. Application development is outsourced.
- C. Source code is escrowed.
- D. Developers have access to production environment.

**Answer: D**

**NEW QUESTION 765**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 769**

- (Exam Topic 2)

Whose risk tolerance matters MOST when making a risk decision?

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

**Answer: C**

**NEW QUESTION 774**

- (Exam Topic 2)

Which of the following is MOST essential for an effective change control environment?

- A. Business management approval of change requests
- B. Separation of development and production environments
- C. Requirement of an implementation rollback plan
- D. IT management review of implemented changes

**Answer: A**

**NEW QUESTION 777**

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 779**

- (Exam Topic 2)

An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Alpha	High	Medium	High
Bravo	High	Low	Medium
Charlie	High	High	High
Delta	High	Medium	Medium

- A. Project Charlie
- B. Project Bravo

- C. Project Alpha
- D. Project Delta

**Answer:** A

**NEW QUESTION 782**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 785**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 786**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 788**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 789**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 793**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 796**

- (Exam Topic 2)

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

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

**Answer:** A

#### **NEW QUESTION 800**

- (Exam Topic 2)

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

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

**Answer:** C

#### **NEW QUESTION 802**

- (Exam Topic 2)

A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

- A. Recommend avoiding the risk.
- B. Validate the risk response with internal audit.
- C. Update the risk register.
- D. Evaluate outsourcing the process.

**Answer:** C

#### **NEW QUESTION 803**

- (Exam Topic 2)

Which of the following is the GREATEST concern associated with business end users developing their own applications on end user spreadsheets and database programs?

- A. An IT project manager is not assigned to oversee development.
- B. Controls are not applied to the applications.
- C. There is a lack of technology recovery options.
- D. The applications are not captured in the risk profile.

**Answer:** C

#### **NEW QUESTION 806**

- (Exam Topic 2)

An organization's risk tolerance should be defined and approved by which of the following?

- A. The chief risk officer (CRO)
- B. The board of directors
- C. The chief executive officer (CEO)
- D. The chief information officer (CIO)

**Answer:** B

#### **NEW QUESTION 809**

- (Exam Topic 2)

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

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

**Answer:** D

#### **NEW QUESTION 811**

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 815

- (Exam Topic 2)

The MAIN purpose of a risk register is to:

- A. document the risk universe of the organization.
- B. promote an understanding of risk across the organization.
- C. enable well-informed risk management decisions.
- D. identify stakeholders associated with risk scenarios.

**Answer: C**

#### NEW QUESTION 819

- (Exam Topic 2)

Which of the following will BEST help to ensure that information system controls are effective?

- A. Responding promptly to control exceptions
- B. Implementing compensating controls
- C. Testing controls periodically
- D. Automating manual controls

**Answer: C**

#### NEW QUESTION 823

- (Exam Topic 2)

A new policy has been published to forbid copying of data onto removable media. Which type of control has been implemented?

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

**Answer: C**

#### NEW QUESTION 828

- (Exam Topic 2)

Which of the following criteria is MOST important when developing a response to an attack that would compromise data?

- A. The recovery time objective (RTO)
- B. The likelihood of a recurring attack
- C. The organization's risk tolerance
- D. The business significance of the information

**Answer: D**

#### NEW QUESTION 829

- (Exam Topic 2)

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

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

**Answer: A**

#### NEW QUESTION 830

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 833

- (Exam Topic 2)

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

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

**Answer: C**

**NEW QUESTION 836**

- (Exam Topic 2)

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

- A. Maturity of the enterprise architecture
- B. Cost of control implementation
- C. Reliability of key performance indicators (KPIs)
- D. Reliability of key risk indicators (KPIs)

**Answer: B**

**NEW QUESTION 837**

- (Exam Topic 2)

Which of the following would be MOST beneficial as a key risk indicator (KRI)?

- A. Current capital allocation reserves
- B. Negative security return on investment (ROI)
- C. Project cost variances
- D. Annualized loss projections

**Answer: D**

**NEW QUESTION 842**

- (Exam Topic 2)

Within the three lines of defense model, the accountability for the system of internal control resides with:

- A. the chief information officer (CIO).
- B. the board of directors
- C. enterprise risk management
- D. the risk practitioner

**Answer: B**

**NEW QUESTION 844**

- (Exam Topic 2)

Which of the following BEST supports the communication of risk assessment results to stakeholders?

- A. Monitoring of high-risk areas
- B. Classification of risk profiles
- C. Periodic review of the risk register
- D. Assignment of risk ownership

**Answer: D**

**NEW QUESTION 845**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 847**

- (Exam Topic 2)

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

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

**Answer: D**

**NEW QUESTION 848**

- (Exam Topic 2)

Which of the following is the BEST indicator of the effectiveness of a control monitoring program?

- A. Time between control failure and failure detection
- B. Number of key controls as a percentage of total control count
- C. Time spent on internal control assessment reviews
- D. Number of internal control failures within the measurement period

**Answer:** A

**NEW QUESTION 852**

- (Exam Topic 2)

Which of the following is the MOST important consideration when performing a risk assessment of a fire suppression system within a data center?

- A. Insurance coverage
- B. Onsite replacement availability
- C. Maintenance procedures
- D. Installation manuals

**Answer:** C

**NEW QUESTION 854**

- (Exam Topic 2)

The BEST criteria when selecting a risk response is the:

- A. capability to implement the response
- B. importance of IT risk within the enterprise
- C. effectiveness of risk response options
- D. alignment of response to industry standards

**Answer:** C

**NEW QUESTION 858**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 863**

- (Exam Topic 2)

Which of the following risk register elements is MOST likely to be updated if the attack surface or exposure of an asset is reduced?

- A. Likelihood rating
- B. Control effectiveness
- C. Assessment approach
- D. Impact rating

**Answer:** A

**NEW QUESTION 866**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 869**

- (Exam Topic 2)

Which of the following is the MOST important objective of embedding risk management practices into the initiation phase of the project management life cycle?

- A. To deliver projects on time and on budget
- B. To assess inherent risk
- C. To include project risk in the enterprise-wide IT risk profile.
- D. To assess risk throughout the project

**Answer:** B

**NEW QUESTION 872**

- (Exam Topic 2)

Business areas within an organization have engaged various cloud service providers directly without assistance from the IT department. What should the risk practitioner do?

- A. Recommend the IT department remove access to the cloud services.

- B. Engage with the business area managers to review controls applied.
- C. Escalate to the risk committee.
- D. Recommend a risk assessment be conducted.

**Answer: B**

**NEW QUESTION 873**

- (Exam Topic 2)

Which of the following provides the MOST important information to facilitate a risk response decision?

- A. Audit findings
- B. Risk appetite
- C. Key risk indicators
- D. Industry best practices

**Answer: B**

**NEW QUESTION 876**

- (Exam Topic 2)

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

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

**Answer: A**

**NEW QUESTION 879**

- (Exam Topic 2)

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

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

**Answer: D**

**NEW QUESTION 883**

- (Exam Topic 2)

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

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

**Answer: B**

**NEW QUESTION 886**

- (Exam Topic 2)

Which of the following BEST confirms the existence and operating effectiveness of information systems controls?

- A. Self-assessment questionnaires completed by management
- B. Review of internal audit and third-party reports
- C. Management review and sign-off on system documentation
- D. First-hand direct observation of the controls in operation

**Answer: B**

**NEW QUESTION 889**

- (Exam Topic 2)

Which of the following is MOST helpful in determining the effectiveness of an organization's IT risk mitigation efforts?

- A. Assigning identification dates for risk scenarios in the risk register
- B. Updating impact assessments for risk scenario
- C. Verifying whether risk action plans have been completed
- D. Reviewing key risk indicators (KRIS)

**Answer: D**

**NEW QUESTION 893**

- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to consider when evaluating plans for changes to IT services?

- A. Change testing schedule
- B. Impact assessment of the change
- C. Change communication plan
- D. User acceptance testing (UAT)

**Answer: B**

#### **NEW QUESTION 898**

- (Exam Topic 2)

A new regulator/ requirement imposes severe fines for data leakage involving customers' personally identifiable information (PII). The risk practitioner has recommended avoiding the risk. Which of the following actions would BEST align with this recommendation?

- A. Reduce retention periods for PII data.
- B. Move PII to a highly-secured outsourced site.
- C. Modify business processes to stop collecting PII.
- D. Implement strong encryption for PII.

**Answer: C**

#### **NEW QUESTION 899**

- (Exam Topic 2)

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

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

**Answer: C**

#### **NEW QUESTION 901**

- (Exam Topic 2)

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

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

**Answer: A**

#### **NEW QUESTION 906**

- (Exam Topic 2)

Which of the following is MOST important to include in a Software as a Service (SaaS) vendor agreement?

- A. An annual contract review
- B. A service level agreement (SLA)
- C. A requirement to adopt an established risk management framework
- D. A requirement to provide an independent audit report

**Answer: B**

#### **NEW QUESTION 910**

- (Exam Topic 2)

For no apparent reason, the time required to complete daily processing for a legacy application is approaching a risk threshold. Which of the following activities should be performed FIRST?

- A. Temporarily increase the risk threshold.
- B. Suspend processing to investigate the problem.
- C. Initiate a feasibility study for a new application.
- D. Conduct a root-cause analysis.

**Answer: D**

#### **NEW QUESTION 913**

- (Exam Topic 2)

An IT license audit has revealed that there are several unlicensed copies of software to be:

- A. immediately uninstall the unlicensed software from the laptops
- B. centralize administration rights on laptops so that installations are controlled
- C. report the issue to management so appropriate action can be taken.
- D. procure the requisite licenses for the software to minimize business impact.

**Answer: B**



**NEW QUESTION 915**

- (Exam Topic 2)

Which of the following is MOST important to enable well-informed cybersecurity risk decisions?

- A. Determine and understand the risk rating of scenarios.
- B. Conduct risk assessment peer reviews.
- C. Identify roles and responsibilities for security controls.
- D. Engage a third party to perform a risk assessment.

**Answer:** A

**NEW QUESTION 918**

- (Exam Topic 2)

An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:

- A. identifying risk scenarios.
- B. determining the risk strategy.
- C. calculating impact and likelihood.
- D. completing the controls catalog.

**Answer:** A

**NEW QUESTION 919**

.....

## 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/>