



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 3)

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

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

Answer: B

NEW QUESTION 2

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 3

- (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 4

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 5

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 6

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 7

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 8

- (Exam Topic 3)

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 9

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 10

- (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 10

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 15

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 20

- (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 25

- (Exam Topic 3)

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

- A. Demonstration that the control is operating as designed
- B. A successful walk-through of the associated risk assessment
- C. Management attestation that the control is operating effectively

D. Automated data indicating that risk has been reduced

Answer: C

NEW QUESTION 27

- (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 28

- (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 31

- (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 33

- (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 38

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 39

- (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 41

- (Exam Topic 3)

In an organization dependent on data analytics to drive decision-making, which of the following would BEST help to minimize the risk associated with inaccurate data?

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

Answer: B

NEW QUESTION 46

- (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 47

- (Exam Topic 3)

Which of the following is the MOST important concern when assigning multiple risk owners for an identified risk?

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

Answer: A

NEW QUESTION 50

- (Exam Topic 3)

After a high-profile systems breach at an organization's key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:

Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

Type	Scope	Completed By
External audit	Financial systems and processes	Third party
Internal audit	IT security risk management	Vendor
Vendor performance scorecard	Service level agreement compliance	Organization
Regulatory examination	Information security management program	Regulator

- A. External audit
- B. Internal audit
- C. Vendor performance scorecard
- D. Regulatory examination

Answer: A

NEW QUESTION 54

- (Exam Topic 3)

Which of the following is a drawback in the use of quantitative risk analysis?

- A. It assigns numeric values to exposures of assets.
- B. It requires more resources than other methods
- C. It produces the results in numeric form.
- D. It is based on impact analysis of information assets.

Answer: B

NEW QUESTION 58

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 59

- (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 62

- (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 66

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 68

- (Exam Topic 3)

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 70

- (Exam Topic 3)

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 74

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 79

- (Exam Topic 3)

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

- A. An established process for project change management
- B. Retention of test data and results for review purposes

- C. Business managements review of functional requirements
- D. Segregation between development, test, and production

Answer: A

NEW QUESTION 80

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 84

- (Exam Topic 3)

Which of the following is the MOST effective way to integrate risk and compliance management?

- A. Embedding risk management into compliance decision-making
- B. Designing corrective actions to improve risk response capabilities
- C. Embedding risk management into processes that are aligned with business drivers
- D. Conducting regular self-assessments to verify compliance

Answer: A

NEW QUESTION 89

- (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 94

- (Exam Topic 3)

An organization practices the principle of least privilege. To ensure access remains appropriate, application owners should be required to review user access rights on a regular basis by obtaining:

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

Answer: B

NEW QUESTION 98

- (Exam Topic 3)

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 102

- (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 106

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 109

- (Exam Topic 3)

Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?

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

Answer: D

NEW QUESTION 110

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 114

- (Exam Topic 3)

Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?

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

Answer: B

NEW QUESTION 117

- (Exam Topic 3)

When a risk practitioner is determining a system's criticality, it is MOST helpful to review the associated:

- A. process flow.
- B. business impact analysis (BIA).
- C. service level agreement (SLA).
- D. system architecture.

Answer: B

NEW QUESTION 121

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 123

- (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 126

- (Exam Topic 3)

Which of the following would be a risk practitioner's BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?

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

Answer: B

NEW QUESTION 127

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 131

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 132

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 135

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 139

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 144

- (Exam Topic 3)

An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?

- A. The volume of risk scenarios is too large
- B. Risk aggregation has not been completed
- C. Risk scenarios are not applicable
- D. The risk analysts for each scenario is incomplete

Answer: C

NEW QUESTION 149

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 154

- (Exam Topic 3)

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

- A. benchmarks against other organizations
- B. defines a qualitative measure of risk
- C. provides a reference for progress
- D. provides risk metrics.

Answer: C

NEW QUESTION 157

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 159

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 160

- (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 165

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 169

- (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 170

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 175

- (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 177

- (Exam Topic 3)

Which of the following is the GREATEST risk associated with the misclassification of data?

- A. inadequate resource allocation
- B. Data disruption
- C. Unauthorized access
- D. Inadequate retention schedules

Answer: A

NEW QUESTION 182

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 184

- (Exam Topic 3)

Which of the following is the PRIMARY role of a data custodian in the risk management process?

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

Answer: D

NEW QUESTION 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 188

- (Exam Topic 3)

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

- A. Board of directors
- B. Vendors
- C. Regulators

D. Legal team

Answer: A

NEW QUESTION 192

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 195

- (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 197

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 198

- (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 199

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 202

- (Exam Topic 3)

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 205

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 208

- (Exam Topic 3)

An organization has experienced several incidents of extended network outages that have exceeded tolerance. Which of the following should be the risk practitioner's FIRST step to address this situation?

- A. Recommend additional controls to address the risk.
- B. Update the risk tolerance level to acceptable thresholds.
- C. Update the incident-related risk trend in the risk register.
- D. Recommend a root cause analysis of the incidents.

Answer: D

NEW QUESTION 212

- (Exam Topic 3)

A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

- A. Monitor the databases for abnormal activity
- B. Approve exception to allow the software to continue operating
- C. Require the software vendor to remediate the vulnerabilities
- D. Accept the risk and let the vendor run the software as is

Answer: C

NEW QUESTION 213

- (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 217

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 221

- (Exam Topic 3)

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

- A. exceeding availability thresholds
- B. experiencing hardware failures
- C. exceeding current patching standards.
- D. meeting the baseline for hardening.

Answer: D

NEW QUESTION 224

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 227

- (Exam Topic 3)

Which of the following is the BEST evidence that risk management is driving business decisions in an organization?

- A. Compliance breaches are addressed in a timely manner.
- B. Risk ownership is identified and assigned.
- C. Risk treatment options receive adequate funding.
- D. Residual risk is within risk tolerance.

Answer: B

NEW QUESTION 229

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 233

- (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 237

- (Exam Topic 3)

An IT risk threat analysis is BEST used to establish

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

Answer: A

NEW QUESTION 238

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 241

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 244

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 245

- (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 249

- (Exam Topic 3)

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 253

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 254

- (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 259

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 260

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 264

- (Exam Topic 3)

Which of the following would MOST likely require a risk practitioner to update the risk register?

- A. An alert being reported by the security operations center.
- B. Development of a project schedule for implementing a risk response
- C. Completion of a project for implementing a new control
- D. Engagement of a third party to conduct a vulnerability scan

Answer:

C

NEW QUESTION 266

- (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 270

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 273

- (Exam Topic 3)

When developing a risk awareness training program, which of the following training topics would BEST facilitate a thorough understanding of risk scenarios?

- A. Mapping threats to organizational objectives
- B. Reviewing past audits
- C. Analyzing key risk indicators (KRIs)
- D. Identifying potential sources of risk

Answer: D

NEW QUESTION 274

- (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 276

- (Exam Topic 3)

Which of the following should be the MOST important consideration when performing a vendor risk assessment?

- A. Results of the last risk assessment of the vendor
- B. Inherent risk of the business process supported by the vendor
- C. Risk tolerance of the vendor
- D. Length of time since the last risk assessment of the vendor

Answer: B

NEW QUESTION 277

- (Exam Topic 3)

All business units within an organization have the same risk response plan for creating local disaster recovery plans. In an effort to achieve cost effectiveness, the BEST course of action would be to:

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

Answer: D

NEW QUESTION 278

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 281

- (Exam Topic 3)

The PRIMARY purpose of IT control status reporting is to:

- A. ensure compliance with IT governance strategy.
- B. assist internal audit in evaluating and initiating remediation efforts.
- C. benchmark IT controls with Industry standards.
- D. facilitate the comparison of the current and desired states.

Answer: A

NEW QUESTION 286

- (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 288

- (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 290

- (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 291

- (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 295

- (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 296

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 301

- (Exam Topic 3)

Which of the following trends would cause the GREATEST concern regarding the effectiveness of an organization's user access control processes? An increase in the:

- A. ratio of disabled to active user accounts.
- B. percentage of users with multiple user accounts.
- C. average number of access entitlements per user account.
- D. average time between user transfers and access updates.

Answer: D

NEW QUESTION 304

- (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 306

- (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 310

- (Exam Topic 3)

The MOST important objective of information security controls is to:

- A. Identify threats and vulnerability
- B. Ensure alignment with industry standards
- C. Provide measurable risk reduction
- D. Enforce strong security solutions

Answer: C

NEW QUESTION 311

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 316

- (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 321

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 322

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 327

- (Exam Topic 3)

What is the PRIMARY reason to periodically review key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 332

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 336

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 339

- (Exam Topic 3)

A risk practitioner has received an updated enterprise risk management (ERM) report showing that residual risk is now within the organization's defined appetite and tolerance levels. Which of the following is the risk practitioner's BEST course of action?

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

Answer: D

NEW QUESTION 342

- (Exam Topic 3)

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

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

Answer:

B

NEW QUESTION 346

- (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 348

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 350

- (Exam Topic 3)

Which of the following is the MOST important technology control to reduce the likelihood of fraudulent payments committed internally?

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

Answer: B

NEW QUESTION 352

- (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 356

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 361

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 366

- (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 371

- (Exam Topic 3)

During a risk assessment, a key external technology supplier refuses to provide control design and effectiveness information, citing confidentiality concerns. What should the risk practitioner do NEXT?

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

Answer: C

NEW QUESTION 372

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 376

- (Exam Topic 3)

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

- A. identify key risk indicators (KRIs) for ongoing monitoring
- B. validate the CTO's decision with the business process owner
- C. update the risk register with the selected risk response
- D. recommend that the CTO revisit the risk acceptance decision.

Answer: A

NEW QUESTION 380

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 383

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 384

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 386

- (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 389

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 394

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 398

- (Exam Topic 3)

Which of the following is the MOST important key performance indicator (KPI) to monitor the effectiveness of disaster recovery processes?

- A. Percentage of IT systems recovered within the mean time to restore (MTTR) during the disaster recovery test
- B. Percentage of issues arising from the disaster recovery test resolved on time
- C. Percentage of IT systems included in the disaster recovery test scope
- D. Percentage of IT systems meeting the recovery time objective (RTO) during the disaster recovery test

Answer: D

NEW QUESTION 403

- (Exam Topic 3)

Which of the following is the BEST way to help ensure risk will be managed properly after a business process has been re-engineered?

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

Answer: A

NEW QUESTION 405

- (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 407

- (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 409

- (Exam Topic 3)

While conducting an organization-wide risk assessment, it is noted that many of the information security policies have not changed in the past three years. The BEST course of action is to:

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

Answer: D

NEW QUESTION 412

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 416

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 418

- (Exam Topic 3)

A department allows multiple users to perform maintenance on a system using a single set of credentials. A risk practitioner determined this practice to be high-risk. Which of the following is the MOST effective way to mitigate this risk?

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

Answer: B

NEW QUESTION 419

- (Exam Topic 3)

Which of the following is the BEST way to assess the effectiveness of an access management process?

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

Answer: B

NEW QUESTION 420

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 425

- (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 427

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 432

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 434

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 436

- (Exam Topic 3)

Which of the following is MOST important when implementing an organization's security policy?

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

Answer: A

NEW QUESTION 439

- (Exam Topic 3)

An organization control environment is MOST effective when:

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

Answer: B

NEW QUESTION 443

- (Exam Topic 3)

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 447

- (Exam Topic 3)

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

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

Answer:

C

NEW QUESTION 449

- (Exam Topic 3)

Which of the following provides the MOST useful information to determine risk exposure following control implementations?

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

Answer: C

NEW QUESTION 450

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 454

- (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 458

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 463

- (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 464

- (Exam Topic 3)

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 466

- (Exam Topic 3)

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

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

D. History of risk events

Answer: B

NEW QUESTION 471

- (Exam Topic 3)

When a high-risk security breach occurs, which of the following would be MOST important to the person responsible for managing the incident?

- A. An analysis of the security logs that illustrate the sequence of events
- B. An analysis of the impact of similar attacks in other organizations
- C. A business case for implementing stronger logical access controls
- D. A justification of corrective action taken

Answer: B

NEW QUESTION 474

- (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 475

- (Exam Topic 3)

An organization has recently been experiencing frequent data corruption incidents. Implementing a file corruption detection tool as a risk response strategy will help to:

- A. reduce the likelihood of future events
- B. restore availability
- C. reduce the impact of future events
- D. address the root cause

Answer: D

NEW QUESTION 480

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 481

- (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 484

- (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 489

- (Exam Topic 3)

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 491

- (Exam Topic 3)

An IT department originally planned to outsource the hosting of its data center at an overseas location to reduce operational expenses. After a risk assessment, the department has decided to keep the data center in-house. How should the risk treatment response be reflected in the risk register?

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

Answer: A

NEW QUESTION 495

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 498

- (Exam Topic 3)

Which of the following provides the MOST useful information when determining if a specific control should be implemented?

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

Answer: B

NEW QUESTION 502

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 504

- (Exam Topic 3)

Which of the following is the PRIMARY objective of providing an aggregated view of IT risk to business management?

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

Answer: B

NEW QUESTION 505

- (Exam Topic 3)

Which of the following BEST enforces access control for an organization that uses multiple cloud technologies?

- A. Senior management support of cloud adoption strategies
- B. Creation of a cloud access risk management policy
- C. Adoption of a cloud access security broker (CASB) solution
- D. Expansion of security information and event management (SIEM) to cloud services

Answer: C

NEW QUESTION 506

- (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 508

- (Exam Topic 3)

Effective risk communication BEST benefits an organization by:

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

Answer: A

NEW QUESTION 510

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 513

- (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 518

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 523

- (Exam Topic 3)

As part of business continuity planning, which of the following is MOST important to include in a business impact analysis (BIA)?

- A. An assessment of threats to the organization
- B. An assessment of recovery scenarios
- C. industry standard framework
- D. Documentation of testing procedures

Answer: A

NEW QUESTION 525

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 530

- (Exam Topic 2)

Which of the following should be the risk practitioner's FIRST course of action when an organization has decided to expand into new product areas?

- A. Identify any new business objectives with stakeholders.
- B. Present a business case for new controls to stakeholders.
- C. Revise the organization's risk and control policy.
- D. Review existing risk scenarios with stakeholders.

Answer: D

NEW QUESTION 534

- (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 535

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 539

- (Exam Topic 2)

A risk practitioner notices a trend of noncompliance with an IT-related control. Which of the following would BEST assist in making a recommendation to management?

- A. Assessing the degree to which the control hinders business objectives
- B. Reviewing the IT policy with the risk owner
- C. Reviewing the roles and responsibilities of control process owners
- D. Assessing noncompliance with control best practices

Answer: A

NEW QUESTION 543

- (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 547

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 548

- (Exam Topic 2)

The MAIN purpose of having a documented risk profile is to:

- A. comply with external and internal requirements.
- B. enable well-informed decision making.
- C. prioritize investment projects.
- D. keep the risk register up-to-date.

Answer:

B

NEW QUESTION 550

- (Exam Topic 2)

The maturity of an IT risk management program is MOST influenced by:

- A. the organization's risk culture
- B. benchmarking results against similar organizations
- C. industry-specific regulatory requirements
- D. expertise available within the IT department

Answer: A

NEW QUESTION 553

- (Exam Topic 2)

Which of the following is MOST critical to the design of relevant risk scenarios?

- A. The scenarios are based on past incidents.
- B. The scenarios are linked to probable organizational situations.
- C. The scenarios are mapped to incident management capabilities.
- D. The scenarios are aligned with risk management capabilities.

Answer: B

NEW QUESTION 557

- (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 562

- (Exam Topic 2)

Which of the following is MOST helpful to review when identifying risk scenarios associated with the adoption of Internet of Things (IoT) technology in an organization?

- A. The business case for the use of IoT
- B. The IoT threat landscape
- C. Policy development for IoT
- D. The network that IoT devices can access

Answer: B

NEW QUESTION 567

- (Exam Topic 2)

Of the following, who should be responsible for determining the inherent risk rating of an application?

- A. Application owner
- B. Senior management
- C. Risk practitioner
- D. Business process owner

Answer: C

NEW QUESTION 569

- (Exam Topic 2)

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

- A. Engaging sponsorship by senior management
- B. Utilizing data and resources internal to the organization
- C. Including input from risk and business unit management
- D. Developing in collaboration with internal audit

Answer: C

NEW QUESTION 572

- (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 577

- (Exam Topic 2)

Which of the following methods would BEST contribute to identifying obscure risk scenarios?

- A. Brainstorming sessions
- B. Control self-assessments
- C. Vulnerability analysis
- D. Monte Carlo analysis

Answer: A

NEW QUESTION 580

- (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 585

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 589

- (Exam Topic 2)

Which of the following would present the GREATEST challenge when assigning accountability for control ownership?

- A. Weak governance structures
- B. Senior management scrutiny
- C. Complex regulatory environment
- D. Unclear reporting relationships

Answer: D

NEW QUESTION 594

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 596

- (Exam Topic 2)

After mapping generic risk scenarios to organizational security policies, the NEXT course of action should be to:

- A. record risk scenarios in the risk register for analysis.
- B. validate the risk scenarios for business applicability.
- C. reduce the number of risk scenarios to a manageable set.
- D. perform a risk analysis on the risk scenarios.

Answer: B

NEW QUESTION 599

- (Exam Topic 2)

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

- A. The scenarios are based on industry best practice.

- B. The scenarios focus on current vulnerabilities.
- C. The scenarios are relevant to the organization.
- D. The scenarios include technical consequences.

Answer: C

NEW QUESTION 604

- (Exam Topic 2)

Which of the following is the BEST indication of the effectiveness of a business continuity program?

- A. Business continuity tests are performed successfully and issues are addressed.
- B. Business impact analyses are reviewed and updated in a timely manner.
- C. Business continuity and disaster recovery plans are regularly updated.
- D. Business units are familiar with the business continuity plans and process.

Answer: A

NEW QUESTION 605

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 607

- (Exam Topic 2)

Which of the following is the BEST way to ensure ongoing control effectiveness?

- A. Establishing policies and procedures
- B. Periodically reviewing control design
- C. Measuring trends in control performance
- D. Obtaining management control attestations

Answer: C

NEW QUESTION 611

- (Exam Topic 2)

What is MOST important for the risk practitioner to understand when creating an initial IT risk register?

- A. Enterprise architecture (EA)
- B. Control environment
- C. IT objectives
- D. Organizational objectives

Answer: D

NEW QUESTION 614

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 617

- (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 619

- (Exam Topic 2)

The PRIMARY purpose of using control metrics is to evaluate the:

- A. amount of risk reduced by compensating controls.
- B. amount of risk present in the organization.
- C. variance against objectives.
- D. number of incidents.

Answer: C

NEW QUESTION 621

- (Exam Topic 2)

Which of the following will BEST help an organization select a recovery strategy for critical systems?

- A. Review the business impact analysis.
- B. Create a business continuity plan.
- C. Analyze previous disaster recovery reports.
- D. Conduct a root cause analysis.

Answer: A

NEW QUESTION 622

- (Exam Topic 2)

Which of the following would BEST help secure online financial transactions from improper users?

- A. Review of log-in attempts
- B. Multi-level authorization
- C. Periodic review of audit trails
- D. Multi-factor authentication

Answer: D

NEW QUESTION 623

- (Exam Topic 2)

Which of the following will be MOST effective to mitigate the risk associated with the loss of company data stored on personal devices?

- A. An acceptable use policy for personal devices
- B. Required user log-on before synchronizing data
- C. Enforced authentication and data encryption
- D. Security awareness training and testing

Answer: C

NEW QUESTION 627

- (Exam Topic 2)

An audit reveals that there are changes in the environment that are not reflected in the risk profile. Which of the following is the BEST course of action?

- A. Review the risk identification process.
- B. Inform the risk scenario owners.
- C. Create a risk awareness communication plan.
- D. Update the risk register.

Answer: A

NEW QUESTION 632

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 633

- (Exam Topic 2)

An IT operations team implements disaster recovery controls based on decisions from application owners regarding the level of resiliency needed. Who is the risk owner in this scenario?

- A. Business resilience manager
- B. Disaster recovery team lead
- C. Application owner
- D. IT operations manager

Answer: C

NEW QUESTION 634

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 635

- (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 637

- (Exam Topic 2)

From a risk management perspective, which of the following is the PRIMARY benefit of using automated system configuration validation tools?

- A. Residual risk is reduced.
- B. Staff costs are reduced.
- C. Operational costs are reduced.
- D. Inherent risk is reduced.

Answer: C

NEW QUESTION 640

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 644

- (Exam Topic 2)

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

- 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 647

- (Exam Topic 2)

Which of the following is the MOST effective way to integrate business risk management with IT operations?

- A. Perform periodic IT control self-assessments.
- B. Require a risk assessment with change requests.
- C. Provide security awareness training.
- D. Perform periodic risk assessments.

Answer: D

NEW QUESTION 652

- (Exam Topic 2)

Which of the following will BEST ensure that information security risk factors are mitigated when developing in-house applications?

- A. Identify information security controls in the requirements analysis
- B. Identify key risk indicators (KRIs) as process output.
- C. Design key performance indicators (KPIs) for security in system specifications.
- D. Include information security control specifications in business cases.

Answer: D

NEW QUESTION 653

- (Exam Topic 2)

It is MOST important for a risk practitioner to have an awareness of an organization's processes in order to:

- A. perform a business impact analysis.
- B. identify potential sources of risk.
- C. establish risk guidelines.
- D. understand control design.

Answer: B

NEW QUESTION 656

- (Exam Topic 2)

Which of the following is MOST helpful in developing key risk indicator (KRI) thresholds?

- A. Loss expectancy information
- B. Control performance predictions
- C. IT service level agreements (SLAs)
- D. Remediation activity progress

Answer: A

NEW QUESTION 659

- (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to update when a software upgrade renders an existing key control ineffective?

- A. Audit engagement letter
- B. Risk profile
- C. IT risk register
- D. Change control documentation

Answer: C

NEW QUESTION 663

- (Exam Topic 2)

Which of the following is MOST helpful to management when determining the resources needed to mitigate a risk?

- A. An internal audit
- B. A heat map
- C. A business impact analysis (BIA)
- D. A vulnerability report

Answer: C

NEW QUESTION 665

- (Exam Topic 2)

A bank is experiencing an increasing incidence of customer identity theft. Which of the following is the BEST way to mitigate this risk?

- A. Implement monitoring techniques.
- B. Implement layered security.
- C. Outsource to a local processor.
- D. Conduct an awareness campaign.

Answer: B

NEW QUESTION 666

- (Exam Topic 2)

Which of the following indicates an organization follows IT risk management best practice?

- A. The risk register template uses an industry standard.
- B. The risk register is regularly updated.
- C. All fields in the risk register have been completed.
- D. Controls are listed against risk entries in the register.

Answer: A

NEW QUESTION 668

- (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 672

- (Exam Topic 2)

An organization has received notification that it is a potential victim of a cybercrime that may have compromised sensitive customer data. What should be The FIRST course of action?

- A. Invoke the incident response plan.
- B. Determine the business impact.
- C. Conduct a forensic investigation.
- D. Invoke the business continuity plan (BCP).

Answer: A

NEW QUESTION 673

- (Exam Topic 2)

A risk practitioner is reviewing the status of an action plan to mitigate an emerging IT risk and finds the risk level has increased. The BEST course of action would be to:

- A. implement the planned controls and accept the remaining risk.
- B. suspend the current action plan in order to reassess the risk.
- C. revise the action plan to include additional mitigating controls.
- D. evaluate whether selected controls are still appropriate.

Answer: D

NEW QUESTION 674

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 678

- (Exam Topic 2)

Which of the following could BEST detect an in-house developer inserting malicious functions into a web-based application?

- A. Segregation of duties
- B. Code review
- C. Change management
- D. Audit modules

Answer: B

NEW QUESTION 682

- (Exam Topic 2)

The PRIMARY reason for establishing various Threshold levels for a set of key risk indicators (KRIs) is to:

- A. highlight trends of developing risk.
- B. ensure accurate and reliable monitoring.
- C. take appropriate actions in a timely manner.
- D. set different triggers for each stakeholder.

Answer: B

NEW QUESTION 683

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 687

- (Exam Topic 2)

An internally developed payroll application leverages Platform as a Service (PaaS) infrastructure from the cloud. Who owns the related data confidentiality risk?

- A. IT infrastructure head
- B. Human resources head
- C. Supplier management head
- D. Application development head

Answer: B

NEW QUESTION 690

- (Exam Topic 2)

Which of the following requirements is MOST important to include in an outsourcing contract to help ensure sensitive data stored with a service provider is secure?

- A. A third-party assessment report of control environment effectiveness must be provided at least annually.
- B. Incidents related to data loss must be reported to the organization immediately after they occur.
- C. Risk assessment results must be provided to the organization at least annually.
- D. A cyber insurance policy must be purchased to cover data loss events.

Answer: A

NEW QUESTION 694

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 699

- (Exam Topic 2)

Which type of cloud computing deployment provides the consumer the GREATEST degree of control over the environment?

- A. Community cloud
- B. Private cloud
- C. Hybrid cloud
- D. Public cloud

Answer: B

NEW QUESTION 700

- (Exam Topic 2)

Which of the following will BEST support management reporting on risk?

- A. Risk policy requirements
- B. A risk register
- C. Control self-assessment
- D. Key performance Indicators

Answer: B

NEW QUESTION 705

- (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 710

- (Exam Topic 2)

Which of the following is the BEST method for identifying vulnerabilities?

- A. Batch job failure monitoring
- B. Periodic network scanning
- C. Annual penetration testing
- D. Risk assessments

Answer: C

NEW QUESTION 715

- (Exam Topic 2)

Which of the following statements BEST describes risk appetite?

- A. The amount of risk an organization is willing to accept
- B. The effective management of risk and internal control environments
- C. Acceptable variation between risk thresholds and business objectives
- D. The acceptable variation relative to the achievement of objectives

Answer: A

NEW QUESTION 717

- (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 722

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 723

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 725

- (Exam Topic 2)

Which of the following is the MOST important component of effective security incident response?

- A. Network time protocol synchronization
- B. Identification of attack sources
- C. Early detection of breaches
- D. A documented communications plan

Answer: C

NEW QUESTION 728

- (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 730

- (Exam Topic 2)

Which of the following provides The BEST information when determining whether to accept residual risk of a critical system to be implemented?

- A. Single loss expectancy (SLE)
- B. Cost of the information system
- C. Availability of additional compensating controls
- D. Potential business impacts are within acceptable levels

Answer:

D

NEW QUESTION 735

- (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 739

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 742

- (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 746

- (Exam Topic 2)

A risk practitioner recently discovered that sensitive data 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. Implement equivalent security in the test environment.
- C. Prevent the use of production data for test purposes
- D. Mask data before being transferred to the test environment.

Answer: B

NEW QUESTION 749

- (Exam Topic 2)

Which of the following is MOST important when discussing risk within an organization?

- A. Adopting a common risk taxonomy
- B. Using key performance indicators (KPIs)
- C. Creating a risk communication policy
- D. Using key risk indicators (KRIs)

Answer: A

NEW QUESTION 754

- (Exam Topic 2)

To help ensure all applicable risk scenarios are incorporated into the risk register, it is MOST important to review the:

- A. risk mitigation approach
- B. cost-benefit analysis.
- C. risk assessment results.
- D. vulnerability assessment results

Answer: C

NEW QUESTION 758

- (Exam Topic 2)

A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?

- A. Reviewing access control lists

- B. Authorizing user access requests
- C. Performing user access recertification
- D. Terminating inactive user access

Answer: B

NEW QUESTION 763

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 767

- (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 771

- (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 774

- (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 775

- (Exam Topic 2)

An organization's HR department has implemented a policy requiring staff members to take a minimum of five consecutive days leave per year to mitigate the risk of malicious insider activities. Which of the following is the BEST key performance indicator (KPI) of the effectiveness of this policy?

- A. Number of malicious activities occurring during staff members leave
- B. Percentage of staff members seeking exception to the policy
- C. Percentage of staff members taking leave according to the policy
- D. Financial loss incurred due to malicious activities during staff members' leave

Answer: B

NEW QUESTION 776

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 779

- (Exam Topic 2)

Which of the following would be the BEST justification to invest in the development of a governance, risk, and compliance (GRC) solution?

- A. Facilitating risk-aware decision making by stakeholders
- B. Demonstrating management commitment to mitigate risk
- C. Closing audit findings on a timely basis
- D. Ensuring compliance to industry standards

Answer: A

NEW QUESTION 783

- (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 784

- (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 789

- (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 792

- (Exam Topic 2)

Which of the following will provide the BEST measure of compliance with IT policies?

- A. Evaluate past policy review reports.
- B. Conduct regular independent reviews.
- C. Perform penetration testing.
- D. Test staff on their compliance responsibilities.

Answer: C

NEW QUESTION 795

- (Exam Topic 2)

A recent audit identified high-risk issues in a business unit though a previous control self-assessment (CSA) had good results. Which of the following is the MOST likely reason for the difference?

- A. The audit had a broader scope than the CSA.
- B. The CSA was not sample-based.
- C. The CSA did not test control effectiveness.
- D. The CSA was compliance-based, while the audit was risk-based.

Answer: D

NEW QUESTION 797

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 798

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 803

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 805

- (Exam Topic 2)

Who is PRIMARILY accountable for risk treatment decisions?

- A. Risk owner
- B. Business manager
- C. Data owner
- D. Risk manager

Answer: A

NEW QUESTION 806

- (Exam Topic 2)

Which of the following is the GREATEST concern when using a generic set of IT risk scenarios for risk analysis?

- A. Quantitative analysis might not be possible.
- B. Risk factors might not be relevant to the organization
- C. Implementation costs might increase.
- D. Inherent risk might not be considered.

Answer: B

NEW QUESTION 810

- (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 811

- (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 814

- (Exam Topic 2)

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

- A. External audit findings

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

Answer: D

NEW QUESTION 819

- (Exam Topic 2)

Which of the following is the GREATEST risk associated with the transition of a sensitive data backup solution from on-premise to a cloud service provider?

- A. More complex test restores
- B. Inadequate service level agreement (SLA) with the provider
- C. More complex incident response procedures
- D. Inadequate data encryption

Answer: D

NEW QUESTION 821

- (Exam Topic 2)

Which of the following is the BEST approach for performing a business impact analysis (BIA) of a supply-chain management application?

- A. Reviewing the organization's policies and procedures
- B. Interviewing groups of key stakeholders
- C. Circulating questionnaires to key internal stakeholders
- D. Accepting IT personnel's view of business issues

Answer: B

NEW QUESTION 823

- (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 825

- (Exam Topic 2)

Which of the following can be interpreted from a single data point on a risk heat map?

- A. Risk tolerance
- B. Risk magnitude
- C. Risk response
- D. Risk appetite

Answer: B

NEW QUESTION 826

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 828

- (Exam Topic 2)

Which of the following is the MOST important reason to create risk scenarios?

- A. To assist with risk identification
- B. To determine risk tolerance
- C. To determine risk appetite
- D. To assist in the development of risk responses

Answer: A

NEW QUESTION 833

- (Exam Topic 2)

Which of the following methods is the BEST way to measure the effectiveness of automated information security controls prior to going live?

- A. Testing in a non-production environment
- B. Performing a security control review
- C. Reviewing the security audit report
- D. Conducting a risk assessment

Answer: A

NEW QUESTION 837

- (Exam Topic 2)

Read" rights to application files in a controlled server environment should be approved by the:

- A. business process owner.
- B. database administrator.
- C. chief information officer.
- D. systems administrator.

Answer: A

NEW QUESTION 840

- (Exam Topic 2)

The GREATEST concern when maintaining a risk register is that:

- A. impacts are recorded in qualitative terms.
- B. executive management does not perform periodic reviews.
- C. IT risk is not linked with IT assets.
- D. significant changes in risk factors are excluded.

Answer: D

NEW QUESTION 842

- (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 845

- (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 846

- (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 850

- (Exam Topic 2)

Which of the following would be MOST relevant to stakeholders regarding ineffective control implementation?

- A. Threat to IT
- B. Number of control failures
- C. Impact on business
- D. Risk ownership

Answer: C

NEW QUESTION 855

- (Exam Topic 2)

A risk practitioner learns that the organization's industry is experiencing a trend of rising security incidents. Which of the following is the BEST course of action?

- A. Evaluate the relevance of the evolving threats.
- B. Review past internal audit results.
- C. Respond to organizational security threats.
- D. Research industry published studies.

Answer: A

NEW QUESTION 858

- (Exam Topic 2)

The risk associated with data loss from a website which contains sensitive customer information is BEST owned by:

- A. the third-party website manager
- B. the business process owner
- C. IT security
- D. the compliance manager

Answer: B

NEW QUESTION 863

- (Exam Topic 2)

When testing the security of an IT system, it is MOST important to ensure that;

- A. tests are conducted after business hours.
- B. operators are unaware of the test.
- C. external experts execute the test.
- D. agreement is obtained from stakeholders.

Answer: D

NEW QUESTION 868

- (Exam Topic 2)

Sensitive data has been lost after an employee inadvertently removed a file from the premises, in violation of organizational policy. Which of the following controls MOST likely failed?

- A. Background checks
- B. Awareness training
- C. User access
- D. Policy management

Answer: C

NEW QUESTION 873

- (Exam Topic 2)

Who is MOST likely to be responsible for the coordination between the IT risk strategy and the business risk strategy?

- A. Chief financial officer
- B. Information security director
- C. Internal audit director
- D. Chief information officer

Answer: B

NEW QUESTION 876

- (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 879

- (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 884

- (Exam Topic 2)

Which of the following is the MOST important objective of regularly presenting the project risk register to the project steering committee?

- A. To allocate budget for resolution of risk issues
- B. To determine if new risk scenarios have been identified
- C. To ensure the project timeline is on target
- D. To track the status of risk mitigation actions

Answer: D

NEW QUESTION 886

- (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 891

- (Exam Topic 2)

An upward trend in which of the following metrics should be of MOST concern?

- A. Number of business change management requests
- B. Number of revisions to security policy
- C. Number of security policy exceptions approved
- D. Number of changes to firewall rules

Answer: C

NEW QUESTION 894

- (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 896

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 898

- (Exam Topic 2)

Which of the following would BEST enable mitigation of newly identified risk factors related to internet of Things (IoT)?

- A. Introducing control procedures early in the life cycle
- B. Implementing IoT device software monitoring
- C. Performing periodic risk assessments of IoT
- D. Performing secure code reviews

Answer: A

NEW QUESTION 900

- (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 904

- (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 907**

- (Exam Topic 2)

Which of the following would prompt changes in key risk indicator (KRI) thresholds?

- A. Changes to the risk register
- B. Changes in risk appetite or tolerance
- C. Modification to risk categories
- D. Knowledge of new and emerging threats

Answer: B**NEW QUESTION 909**

- (Exam Topic 2)

Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?

- A. A companion of risk assessment results to the desired state
- B. A quantitative presentation of risk assessment results
- C. An assessment of organizational maturity levels and readiness
- D. A qualitative presentation of risk assessment results

Answer: D**NEW QUESTION 914**

- (Exam Topic 2)

The purpose of requiring source code escrow in a contractual agreement is to:

- A. ensure that the source code is valid and exists.
- B. ensure that the source code is available if the vendor ceases to exist.
- C. review the source code for adequacy of controls.
- D. ensure the source code is available when bugs occur.

Answer: B**NEW QUESTION 918**

.....

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/>