



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)

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 2

- (Exam Topic 3)

What are the MOST essential attributes of an effective Key control indicator (KCI)?

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

Answer: B

NEW QUESTION 3

- (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 4

- (Exam Topic 3)

The following is the snapshot of a recently approved IT risk register maintained by an organization's information security department.

Risk ID	Risk Title	Risk Description	Risk Submitter	Risk Owner	Control Owner(s)	Risk Likelihood Rating	Risk Impact Rating	Risk Exposure	Risk Response Type	Risk Response Description
R001	Mobile Data Theft	Laptops and mobile devices can be lost or stolen leading to data compromise	Risk Council	End-User Computing Manager AND Inventory	IT Operations Manager AND Security Operations Manager	Low Likelihood	Very Serious	0.120	Mitigate	Purchase and acquire data encryption software for mobile devices
R003	Fire Hazard	A fire accident may destroy data center equipment and servers leading to loss of availability and services	Information Security Department	Data Center Facilities Manager	Facilities Manager	Low Likelihood	Serious	0.060	Transfer	Buy fire hazard insurance policy
Significant		A disgruntled				0.10	Low Likelihood			0.30
Serious						0.20	Likely			0.50
Very Serious						0.40	Highly Likely			0.70
Catastrophic						0.80	Near Certainty			0.90

After implementing countermeasures listed in "Risk Response Descriptions" for each of the Risk IDs, which of the following component of the register MUST change?

- A. Risk Impact Rating
- B. Risk Owner
- C. Risk Likelihood Rating
- D. Risk Exposure

Answer: B

NEW QUESTION 5

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 6

- (Exam Topic 3)

Which of the following is 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 7

- (Exam Topic 3)

Days before the realization of an acquisition, a data breach is discovered at the company to be acquired. For the accruing organization, this situation represents which of the following?

- A. Threat event
- B. Inherent risk
- C. Risk event
- D. Security incident

Answer: B

NEW QUESTION 8

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 9

- (Exam Topic 3)

During implementation of an intrusion detection system (IDS) to monitor network traffic, a high number of alerts is reported. The risk practitioner should recommend to:

- A. reset the alert threshold based on peak traffic
- B. analyze the traffic to minimize the false negatives
- C. analyze the alerts to minimize the false positives
- D. sniff the traffic using a network analyzer

Answer: C

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 10

- (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 12

- (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 13

- (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 18

- (Exam Topic 3)

Which of the following issues should be of GREATEST concern when evaluating existing controls during a risk assessment?

- A. A high number of approved exceptions exist with compensating controls.
- B. Successive assessments have the same recurring vulnerabilities.
- C. Redundant compensating controls are in place.
- D. Asset custodians are responsible for defining controls instead of asset owners.

Answer: B

NEW QUESTION 21

- (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 22

- (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 25

- (Exam Topic 3)

When developing risk scenario using a list of generic scenarios based on industry best practices, it is MOST imported to:

- A. Assess generic risk scenarios with business users.
- B. Validate the generic risk scenarios for relevance.
- C. Select the maximum possible risk scenarios from the list.
- D. Identify common threats causing generic risk scenarios

Answer: B

NEW QUESTION 29

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 33

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 38

- (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 43

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 44

- (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 49

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 51

- (Exam Topic 3)

During an acquisition, which of the following would provide the MOST useful input to the parent company's risk practitioner when developing risk scenarios for the post-acquisition phase?

- A. Risk management framework adopted by each company
- B. Risk registers of both companies
- C. IT balanced scorecard of each company
- D. Most recent internal audit findings from both companies

Answer: C

NEW QUESTION 56

- (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 58

- (Exam Topic 3)

Which of the following BEST facilitates the alignment of IT risk management with enterprise risk management (ERM)?

- A. Adopting qualitative enterprise risk assessment methods
- B. Linking IT risk scenarios to technology objectives
- C. linking IT risk scenarios to enterprise strategy
- D. Adopting quantitative enterprise risk assessment methods

Answer: C

NEW QUESTION 59

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 64

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 65

- (Exam Topic 3)

Which of the following management action will MOST likely change the likelihood rating of a risk scenario related to remote network access?

- A. Updating the organizational policy for remote access
- B. Creating metrics to track remote connections
- C. Implementing multi-factor authentication
- D. Updating remote desktop software

Answer: A

NEW QUESTION 69

- (Exam Topic 3)

An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course of action?

- A. Report the observation to the chief risk officer (CRO).
- B. Validate the adequacy of the implemented risk mitigation measures.
- C. Update the risk register with the implemented risk mitigation actions.
- D. Revert the implemented mitigation measures until approval is obtained

Answer: B

NEW QUESTION 74

- (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 75

- (Exam Topic 3)

A risk practitioner has been asked to advise management on developing a log collection and correlation strategy. Which of the following should be the MOST important consideration when developing this strategy?

- A. Ensuring time synchronization of log sources.
- B. Ensuring the inclusion of external threat intelligence log sources.
- C. Ensuring the inclusion of all computing resources as log sources.
- D. Ensuring read-write access to all log sources

Answer: A

NEW QUESTION 78

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 82

- (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 87

- (Exam Topic 3)

Recovery the objectives (RTOs) should be based on

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

Answer: C

NEW QUESTION 90

- (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 95

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 97

- (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 98

- (Exam Topic 3)

Which of the following would be MOST helpful to a risk practitioner when ensuring that mitigated risk remains within acceptable limits?

- A. Building an organizational risk profile after updating the risk register
- B. Ensuring risk owners participate in a periodic control testing process
- C. Designing a process for risk owners to periodically review identified risk
- D. Implementing a process for ongoing monitoring of control effectiveness

Answer: D

NEW QUESTION 103

- (Exam Topic 3)

Which of the following should be the PRIMARY goal of developing information security metrics?

- A. Raising security awareness
- B. Enabling continuous improvement
- C. Identifying security threats
- D. Ensuring regulatory compliance

Answer: B

NEW QUESTION 104

- (Exam Topic 3)

Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

- A. Perform a return on investment analysis.
- B. Review the risk register and risk scenarios.
- C. Calculate annualized loss expectancy of risk scenarios.
- D. Raise the maturity of organizational risk management.

Answer: D

NEW QUESTION 107

- (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 108

- (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 109

- (Exam Topic 3)

Which of the following MUST be updated to maintain an IT risk register?

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

Answer: C

NEW QUESTION 112

- (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 116

- (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 120

- (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 122

- (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 123

- (Exam Topic 3)

Following an acquisition, the acquiring company's risk practitioner has been asked to update the organization's IT risk profile What is the MOST important information to review from the acquired company to facilitate this task?

- A. Internal and external audit reports
- B. Risk disclosures in financial statements
- C. Risk assessment and risk register
- D. Business objectives and strategies

Answer: C

NEW QUESTION 125

- (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 128

- (Exam Topic 3)

A deficient control has been identified which could result in great harm to an organization should a low frequency threat event occur. When communicating the associated risk to senior management the risk practitioner should explain:

- A. mitigation plans for threat events should be prepared in the current planning period.
- B. this risk scenario is equivalent to more frequent but lower impact risk scenarios.
- C. the current level of risk is within tolerance.
- D. an increase in threat events could cause a loss sooner than anticipated.

Answer: A

NEW QUESTION 131

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 135

- (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 138

- (Exam Topic 3)

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

- A. KRI design must precede definition of KCIs.
- B. KCIs and KRIs are independent indicators and do not impact each other.
- C. A decreasing trend of KRI readings will lead to changes to KCIs.
- D. Both KRIs and KCIs provide insight to potential changes in the level of risk.

Answer: A

NEW QUESTION 139

- (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 140

- (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 144

- (Exam Topic 3)

The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:

- A. the proposed controls are implemented as scheduled.
- B. security controls are tested prior to implementation.
- C. compliance with corporate policies.
- D. the risk response strategy has been decided.

Answer: A

NEW QUESTION 149

- (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 151

- (Exam Topic 3)

Which of the following is MOST important to promoting a risk-aware culture?

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

Answer: D

NEW QUESTION 153

- (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 154

- (Exam Topic 3)

Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?

- A. Obtain objective assessment of the control environment.
- B. Ensure the risk profile is defined and communicated.
- C. Validate the threat management process.
- D. Obtain an objective view of process gaps and systemic errors.

Answer: A

NEW QUESTION 155

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 156

- (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 158

- (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 162

- (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 166

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 167

- (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 169

- (Exam Topic 3)

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

- A. Control self-assessment (CSA)
- B. Risk policy requirements
- C. A risk register
- D. Key performance indicators (KPIs)

Answer: C

NEW QUESTION 172

- (Exam Topic 3)

When reporting on the performance of an organization's control environment including which of the following would BEST inform stakeholders risk decision-making?

- A. The audit plan for the upcoming period
- B. Spend to date on mitigating control implementation
- C. A report of deficiencies noted during controls testing
- D. A status report of control deployment

Answer: C

NEW QUESTION 176

- (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 178

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 182

- (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 183

- (Exam Topic 2)

The PRIMARY purpose of vulnerability assessments is to:

- A. provide clear evidence that the system is sufficiently secure.
- B. determine the impact of potential threats.
- C. test intrusion detection systems (IDS) and response procedures.
- D. detect weaknesses that could lead to system compromise.

Answer: D

NEW QUESTION 188

- (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 189

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 194

- (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 199

- (Exam Topic 2)

The BEST way to demonstrate alignment of the risk profile with business objectives is through:

- A. risk scenarios.
- B. risk tolerance.
- C. risk policy.
- D. risk appetite.

Answer: B

NEW QUESTION 200

- (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 203

- (Exam Topic 2)

Which of the following will BEST help ensure that risk factors identified during an information systems review are addressed?

- A. Informing business process owners of the risk
- B. Reviewing and updating the risk register
- C. Assigning action items and deadlines to specific individuals
- D. Implementing new control technologies

Answer: C

NEW QUESTION 205

- (Exam Topic 2)

Which of the following is the BEST way to identify changes in the risk profile of an organization?

- A. Monitor key risk indicators (KRIs).
- B. Monitor key performance indicators (KPIs).
- C. Interview the risk owner.
- D. Conduct a gap analysis

Answer: D

NEW QUESTION 210

- (Exam Topic 2)

Which of the following should an organization perform to forecast the effects of a disaster?

- A. Develop a business impact analysis (BIA).
- B. Define recovery time objectives (RTO).
- C. Analyze capability maturity model gaps.
- D. Simulate a disaster recovery.

Answer: A

NEW QUESTION 213

- (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 217

- (Exam Topic 2)

Which of the following should be considered FIRST when assessing risk associated with the adoption of emerging technologies?

- A. Organizational strategy
- B. Cost-benefit analysis
- C. Control self-assessment (CSA)
- D. Business requirements

Answer: A

NEW QUESTION 221

- (Exam Topic 2)

Which of the following is the MOST important reason to revisit a previously accepted risk?

- A. To update risk ownership
- B. To review the risk acceptance with new stakeholders
- C. To ensure risk levels have not changed
- D. To ensure controls are still operating effectively

Answer: C

NEW QUESTION 224

- (Exam Topic 2)

Which of the following is MOST important to the effective monitoring of key risk indicators (KRIS)?

- A. Updating the threat inventory with new threats
- B. Automating log data analysis
- C. Preventing the generation of false alerts
- D. Determining threshold levels

Answer: D

NEW QUESTION 229

- (Exam Topic 2)

Which of the following statements in an organization's current risk profile report is cause for further action by senior management?

- A. Key performance indicator (KPI) trend data is incomplete.
- B. New key risk indicators (KRIs) have been established.
- C. Key performance indicators (KPIs) are outside of targets.
- D. Key risk indicators (KRIs) are lagging.

Answer: B

NEW QUESTION 230

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 235

- (Exam Topic 2)

A risk practitioner observes that the fraud detection controls in an online payment system do not perform as expected. Which of the following will MOST likely change as a result?

- A. Impact
- B. Residual risk
- C. Inherent risk
- D. Risk appetite

Answer: B

NEW QUESTION 236

- (Exam Topic 2)

Following a review of a third-party vendor, it is MOST important for an organization to ensure:

- A. results of the review are accurately reported to management.
- B. identified findings are reviewed by the organization.
- C. results of the review are validated by internal audit.
- D. identified findings are approved by the vendor.

Answer: A

NEW QUESTION 241

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 244

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk responses have been executed according to their risk action plans?

- A. Risk policy review
- B. Business impact analysis (BIA)
- C. Control catalog
- D. Risk register

Answer: D

NEW QUESTION 247

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 248

- (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 252

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 256

- (Exam Topic 2)

Which of the following is the PRIMARY reason for an organization to ensure the risk register is updated regularly?

- A. Risk assessment results are accessible to senior management and stakeholders.
- B. Risk mitigation activities are managed and coordinated.
- C. Key risk indicators (KRIs) are evaluated to validate they are still within the risk threshold.
- D. Risk information is available to enable risk-based decisions.

Answer: D

NEW QUESTION 260

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 263

- (Exam Topic 2)

What should a risk practitioner do FIRST upon learning a risk treatment owner has implemented a different control than what was specified in the IT risk action plan?

- A. Seek approval from the control owner.
- B. Update the action plan in the risk register.
- C. Reassess the risk level associated with the new control.
- D. Validate that the control has an established testing method.

Answer: C

NEW QUESTION 267

- (Exam Topic 2)

Which of the following presents the GREATEST challenge for an IT risk practitioner who wants to report on trends in historical IT risk levels?

- A. Qualitative measures for potential loss events
- B. Changes in owners for identified IT risk scenarios
- C. Changes in methods used to calculate probability
- D. Frequent use of risk acceptance as a treatment option

Answer: A

NEW QUESTION 272

- (Exam Topic 2)

Which of the following is the MOST important consideration when identifying stakeholders to review risk scenarios developed by a risk analyst? The reviewers are:

- A. accountable for the affected processes.
- B. members of senior management.
- C. authorized to select risk mitigation options.
- D. independent from the business operations.

Answer: D

NEW QUESTION 274

- (Exam Topic 2)

A risk practitioner is reporting on an increasing trend of ransomware attacks in the industry. Which of the following information is MOST important to include to enable an informed response decision by key stakeholders?

- A. Methods of attack progression
- B. Losses incurred by industry peers
- C. Most recent antivirus scan reports
- D. Potential impact of events

Answer: D

NEW QUESTION 278

- (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 283

- (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 284

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 285

- (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 287

- (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 288

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 289

- (Exam Topic 2)

An organization has outsourced its backup and recovery procedures to a third-party cloud provider. Which of the following is the risk practitioner s BEST course of action?

- A. Accept the risk and document contingency plans for data disruption.
- B. Remove the associated risk scenario from the risk register due to avoidance.
- C. Mitigate the risk with compensating controls enforced by the third-party cloud provider.
- D. Validate the transfer of risk and update the register to reflect the change.

Answer: C

NEW QUESTION 293

- (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 295

- (Exam Topic 2)

Which of the following is a detective control?

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

Answer: B

NEW QUESTION 298

- (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 303

- (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 308

- (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 313

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 315

- (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 317

- (Exam Topic 2)

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

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

- A. Project Charlie
- B. Project Bravo
- C. Project Alpha
- D. Project Delta

Answer: A

NEW QUESTION 322

- (Exam Topic 2)

Which of the following is the MOST effective way to help ensure an organization's current risk scenarios are relevant?

- A. Adoption of industry best practices
- B. Involvement of stakeholders in risk assessment
- C. Review of risk scenarios by independent parties
- D. Documentation of potential risk in business cases

Answer: B

NEW QUESTION 323

- (Exam Topic 2)

The MOST significant benefit of using a consistent risk ranking methodology across an organization is that it enables:

- A. allocation of available resources
- B. clear understanding of risk levels
- C. assignment of risk to the appropriate owners
- D. risk to be expressed in quantifiable terms

Answer: B

NEW QUESTION 328

- (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 333

- (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 338

- (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 343

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 346

- (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 348

- (Exam Topic 2)

Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?

- A. The KRIs' source data lacks integrity.
- B. The KRIs are not automated.
- C. The KRIs are not quantitative.
- D. The KRIs do not allow for trend analysis.

Answer: A

NEW QUESTION 353

- (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 358

- (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 361

- (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 363

- (Exam Topic 2)

An organization striving to be on the leading edge in regard to risk monitoring would MOST likely implement:

- A. procedures to monitor the operation of controls.
- B. a tool for monitoring critical activities and controls.
- C. real-time monitoring of risk events and control exceptions.
- D. monitoring activities for all critical assets.
- E. Perform a controls assessment.

Answer: C

NEW QUESTION 366

- (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 370

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 371

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 372

- (Exam Topic 2)

An organization is unable to implement a multi-factor authentication requirement until the next fiscal year due to budget constraints. Consequently, a policy exception must be submitted. Which of the following is MOST important to include in the analysis of the exception?

- A. Sections of the policy that may justify not implementing the requirement
- B. Risk associated with the inability to implement the requirement
- C. Budget justification to implement the new requirement during the current year
- D. Industry best practices with respect to implementation of the proposed control

Answer: B

NEW QUESTION 373

- (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 374

- (Exam Topic 2)

To minimize risk in a software development project, when is the BEST time to conduct a risk analysis?

- A. During the business requirement definitions phase
- B. Before periodic steering committee meetings
- C. At each stage of the development life cycle
- D. During the business case development

Answer: A

NEW QUESTION 377

- (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 380

- (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 384

- (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 385

- (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 386

- (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 389

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 392

- (Exam Topic 2)

An organization has introduced risk ownership to establish clear accountability for each process. To ensure effective risk ownership, it is MOST important that:

- A. senior management has oversight of the process.
- B. process ownership aligns with IT system ownership.
- C. segregation of duties exists between risk and process owners.
- D. risk owners have decision-making authority.

Answer: A

NEW QUESTION 395

- (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 397

- (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 399

- (Exam Topic 2)

A risk owner has accepted a high-impact risk because the control was adversely affecting process efficiency. Before updating the risk register, it is MOST important for the risk practitioner to:

- A. ensure suitable insurance coverage is purchased.
- B. negotiate with the risk owner on control efficiency.
- C. reassess the risk to confirm the impact.
- D. obtain approval from senior management.

Answer: D

NEW QUESTION 400

- (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 404

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 405

- (Exam Topic 2)

A control owner has completed a year-long project To strengthen existing controls. It is MOST important for the risk practitioner to:

- A. update the risk register to reflect the correct level of residual risk.
- B. ensure risk monitoring for the project is initiated.
- C. conduct and document a business impact analysis (BIA).
- D. verify cost-benefit of the new controls being implemented.

Answer: A

NEW QUESTION 408

- (Exam Topic 2)

The BEST criteria when selecting a risk response is the:

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

Answer: C

NEW QUESTION 413

- (Exam Topic 2)

The PRIMARY goal of a risk management program is to:

- A. facilitate resource availability.
- B. help ensure objectives are met.
- C. safeguard corporate assets.
- D. help prevent operational losses.

Answer: D

NEW QUESTION 418

- (Exam Topic 2)

IT stakeholders have asked a risk practitioner for IT risk profile reports associated with specific departments to allocate resources for risk mitigation. The BEST way to address this request would be to use:

- A. the cost associated with each control.
- B. historical risk assessments.
- C. key risk indicators (KRIs).
- D. information from the risk register.

Answer: D

NEW QUESTION 422

- (Exam Topic 2)

What can be determined from the risk scenario chart?

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

- A. Relative positions on the risk map
- B. Risk treatment options
- C. Capability of enterprise to implement
- D. The multiple risk factors addressed by a chosen response

Answer: A

NEW QUESTION 426

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 428

- (Exam Topic 3)

Which of the following would be MOST helpful to an information security management team when allocating resources to mitigate exposures?

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

Answer: C

NEW QUESTION 433

- (Exam Topic 3)

An organization has been notified that a disgruntled, terminated IT administrator has tried to break into the corporate network. Which of the following discoveries should be of GREATEST concern to the organization?

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

Answer: A

NEW QUESTION 435

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 437

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 440

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 445

- (Exam Topic 3)

Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?

- A. Percentage of high-risk vulnerabilities missed
- B. Number of high-risk vulnerabilities outstanding
- C. Defined thresholds for high-risk vulnerabilities
- D. Percentage of high-risk vulnerabilities addressed

Answer: D

NEW QUESTION 446

- (Exam Topic 3)

A risk practitioner is preparing a report to communicate changes in the risk and control environment. The BEST way to engage stakeholder attention is to:

- A. include detailed deviations from industry benchmarks,
- B. include a summary linking information to stakeholder needs,
- C. include a roadmap to achieve operational excellence,
- D. publish the report on-demand for stakeholders.

Answer: B

NEW QUESTION 448

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 451

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 452

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 457

- (Exam Topic 3)

Which of the following data would be used when performing a business impact analysis (BIA)?

- A. Cost-benefit analysis of running the current business
- B. Cost of regulatory compliance
- C. Projected impact of current business on future business
- D. Expected costs for recovering the business

Answer: D

NEW QUESTION 460

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 462

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 463

- (Exam Topic 3)

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

- A. Updating the risk register to include the risk mitigation plan
- B. Determining processes for monitoring the effectiveness of the controls

- C. Ensuring that control design reduces risk to an acceptable level
- D. Confirming to management the controls reduce the likelihood of the risk

Answer: A

NEW QUESTION 467

- (Exam Topic 3)

The risk associated with an asset after controls are applied can be expressed as:

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

Answer: C

NEW QUESTION 472

- (Exam Topic 3)

A core data center went offline abruptly for several hours affecting many transactions across multiple locations. Which of the following would provide the MOST useful information to determine mitigating controls?

- A. Forensic analysis
- B. Risk assessment
- C. Root cause analysis
- D. Business impact analysis (BIA)

Answer: A

NEW QUESTION 476

- (Exam Topic 3)

Which of the following is the MOST important objective of an enterprise risk management (ERM) program?

- A. To create a complete repository of risk to the organization
- B. To create a comprehensive view of critical risk to the organization
- C. To provide a bottom-up view of the most significant risk scenarios
- D. To optimize costs of managing risk scenarios in the organization

Answer: B

NEW QUESTION 478

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 483

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 487

- (Exam Topic 2)

Which of the following should be included in a risk assessment report to BEST facilitate senior management's understanding of the results?

- A. Benchmarking parameters likely to affect the results
- B. Tools and techniques used by risk owners to perform the assessments
- C. A risk heat map with a summary of risk identified and assessed
- D. The possible impact of internal and external risk factors on the assessment results

Answer: C

NEW QUESTION 492

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 493

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 494

- (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 499

- (Exam Topic 2)

When updating a risk register with the results of an IT risk assessment, the risk practitioner should log:

- A. high impact scenarios.
- B. high likelihood scenarios.
- C. treated risk scenarios.
- D. known risk scenarios.

Answer: D

NEW QUESTION 503

- (Exam Topic 2)

Which of the following is the PRIMARY responsibility of the first line of defense related to computer-enabled fraud?

- A. Providing oversight of risk management processes
- B. Implementing processes to detect and deter fraud
- C. Ensuring that risk and control assessments consider fraud
- D. Monitoring the results of actions taken to mitigate fraud

Answer: B

NEW QUESTION 506

- (Exam Topic 2)

Which of the following is MOST important to review when determining whether a potential IT service provider's control environment is effective?

- A. Independent audit report
- B. Control self-assessment
- C. MOST important to update when an
- D. Service level agreements (SLAs)

Answer: A

NEW QUESTION 507

- (Exam Topic 2)

Which of the following is the FIRST step when developing a business case to drive the adoption of a risk remediation project by senior management?

- A. Calculating the cost
- B. Analyzing cost-effectiveness
- C. Determining the stakeholders
- D. Identifying the objectives

Answer: A

NEW QUESTION 510

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 514

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 517

- (Exam Topic 2)

Which of the following activities should be performed FIRST when establishing IT risk management processes?

- A. Collect data of past incidents and lessons learned.
- B. Conduct a high-level risk assessment based on the nature of business.
- C. Identify the risk appetite of the organization.
- D. Assess the goals and culture of the organization.

Answer: D

NEW QUESTION 521

- (Exam Topic 1)

Which of the following would be a risk practitioners BEST recommendation for preventing cyber intrusion?

- A. Establish a cyber response plan
- B. Implement data loss prevention (DLP) tools.
- C. Implement network segregation.
- D. Strengthen vulnerability remediation efforts.

Answer: D

NEW QUESTION 525

- (Exam Topic 1)

An organization delegates its data processing to the internal IT team to manage information through its applications. Which of the following is the role of the internal IT team in this situation?

- A. Data controllers
- B. Data processors
- C. Data custodians
- D. Data owners

Answer: B

NEW QUESTION 526

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 529

- (Exam Topic 1)

A risk practitioner has observed that there is an increasing trend of users sending sensitive information by email without using encryption. Which of the following would be the MOST effective approach to mitigate the risk associated with data loss?

- A. Implement a tool to create and distribute violation reports
- B. Raise awareness of encryption requirements for sensitive data.
- C. Block unencrypted outgoing emails which contain sensitive data.
- D. Implement a progressive disciplinary process for email violations.

Answer: C

NEW QUESTION 533

- (Exam Topic 1)

A risk practitioner is assisting with the preparation of a report on the organization's disaster recovery (DR) capabilities. Which information would have the MOST impact on the overall recovery profile?

- A. The percentage of systems meeting recovery target times has increased.
- B. The number of systems tested in the last year has increased.
- C. The number of systems requiring a recovery plan has increased.
- D. The percentage of systems with long recovery target times has decreased.

Answer: D

NEW QUESTION 537

- (Exam Topic 1)

Which of the following is the BEST way to validate the results of a vulnerability assessment?

- A. Perform a penetration test.
- B. Review security logs.
- C. Conduct a threat analysis.
- D. Perform a root cause analysis.

Answer: A

NEW QUESTION 539

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 541

- (Exam Topic 1)

Which of the following controls will BEST detect unauthorized modification of data by a database administrator?

- A. Reviewing database access rights
- B. Reviewing database activity logs
- C. Comparing data to input records
- D. Reviewing changes to edit checks

Answer: B

NEW QUESTION 542

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 547

- (Exam Topic 1)

An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?

- A. Perform a risk assessment
- B. Disable user access.
- C. Develop an access control policy.
- D. Perform root cause analysis.

Answer: B

NEW QUESTION 551

- (Exam Topic 1)

Periodically reviewing and updating a risk register with details on identified risk factors PRIMARILY helps to:

- A. minimize the number of risk scenarios for risk assessment.
- B. aggregate risk scenarios identified across different business units.
- C. build a threat profile of the organization for management review.
- D. provide a current reference to stakeholders for risk-based decisions.

Answer:

C

NEW QUESTION 554

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 556

- (Exam Topic 1)

Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?

- A. Assess the vulnerability management process.
- B. Conduct a control self-assessment.
- C. Conduct a vulnerability assessment.
- D. Reassess the inherent risk of the target.

Answer: A

NEW QUESTION 557

- (Exam Topic 1)

Which of the following should be the PRIMARY input when designing IT controls?

- A. Benchmark of industry standards
- B. Internal and external risk reports
- C. Recommendations from IT risk experts
- D. Outcome of control self-assessments

Answer: B

NEW QUESTION 559

- (Exam Topic 1)

Whether the results of risk analyses should be presented in quantitative or qualitative terms should be based PRIMARILY on the:

- A. requirements of management.
- B. specific risk analysis framework being used.
- C. organizational risk tolerance
- D. results of the risk assessment.

Answer: A

NEW QUESTION 562

- (Exam Topic 1)

Which of the following is the BEST way to determine the ongoing efficiency of control processes?

- A. Perform annual risk assessments.
- B. Interview process owners.
- C. Review the risk register.
- D. Analyze key performance indicators (KPIs).

Answer: D

NEW QUESTION 566

- (Exam Topic 1)

Which of the following will BEST help mitigate the risk associated with malicious functionality in outsourced application development?

- A. Perform an m-depth code review with an expert
- B. Validate functionality by running in a test environment
- C. Implement a service level agreement.
- D. Utilize the change management process.

Answer: C

NEW QUESTION 567

- (Exam Topic 1)

Which of the following is the BEST method to ensure a terminated employee's access to IT systems is revoked upon departure from the organization?

- A. Login attempts are reconciled to a list of terminated employees.

- B. A list of terminated employees is generated for reconciliation against current IT access.
- C. A process to remove employee access during the exit interview is implemented.
- D. The human resources (HR) system automatically revokes system access.

Answer: D

NEW QUESTION 569

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 570

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 571

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 573

- (Exam Topic 1)

Which of the following is the MOST important foundational element of an effective three lines of defense model for an organization?

- A. A robust risk aggregation tool set
- B. Clearly defined roles and responsibilities
- C. A well-established risk management committee
- D. Well-documented and communicated escalation procedures

Answer: B

NEW QUESTION 577

- (Exam Topic 1)

A systems interruption has been traced to a personal USB device plugged into the corporate network by an IT employee who bypassed internal control procedures. Of the following, who should be accountable?

- A. Business continuity manager (BCM)
- B. Human resources manager (HRM)
- C. Chief risk officer (CRO)
- D. Chief information officer (CIO)

Answer: D

NEW QUESTION 580

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 583

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 584

- (Exam Topic 1)

Which of the following BEST provides an early warning that network access of terminated employees is not being revoked in accordance with the service level agreement (SLA)?

- A. Updating multi-factor authentication
- B. Monitoring key access control performance indicators
- C. Analyzing access control logs for suspicious activity
- D. Revising the service level agreement (SLA)

Answer: B

NEW QUESTION 586

- (Exam Topic 1)

A risk practitioner observes that hardware failure incidents have been increasing over the last few months. However, due to built-in redundancy and fault-tolerant architecture, there have been no interruptions to business operations. The risk practitioner should conclude that:

- A. a root cause analysis is required
- B. controls are effective for ensuring continuity
- C. hardware needs to be upgraded
- D. no action is required as there was no impact

Answer: A

NEW QUESTION 587

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 592

- (Exam Topic 1)

A contract associated with a cloud service provider MUST include:

- A. ownership of responsibilities.
- B. a business recovery plan.
- C. provision for source code escrow.
- D. the providers financial statements.

Answer: A

NEW QUESTION 594

- (Exam Topic 1)

An organization is planning to engage a cloud-based service provider for some of its data-intensive business processes. Which of the following is MOST important to help define the IT risk associated with this outsourcing activity?

- A. Service level agreement
- B. Customer service reviews
- C. Scope of services provided
- D. Right to audit the provider

Answer: D

NEW QUESTION 598

- (Exam Topic 1)

The acceptance of control costs that exceed risk exposure is MOST likely an example of:

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

Answer: D

NEW QUESTION 599

- (Exam Topic 1)

Risk mitigation procedures should include:

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

Answer: B

NEW QUESTION 603

.....

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/>