

Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control



NEW QUESTION 1

- (Exam Topic 3)

Which of the following would be a risk practitioner's BEST course of action when a project team has accepted a risk outside the established risk appetite?

- A. Reject the risk acceptance and require mitigating controls.
- B. Monitor the residual risk level of the accepted risk.
- C. Escalate the risk decision to the project sponsor for review.
- D. Document the risk decision in the project risk register.

Answer: B

NEW QUESTION 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)

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 4

- (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 5

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 6

- (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				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 7

- (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 8

- (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 9

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 10

- (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 10

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 12

- (Exam Topic 3)

Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?

- A. Analyzing cyber intelligence reports
- B. Engaging independent cybersecurity consultants
- C. Increasing the frequency of updates to the risk register
- D. Reviewing the outcome of the latest security risk assessment

Answer: D

NEW QUESTION 14

- (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 16

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 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 25

- (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 30

- (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 34

- (Exam Topic 3)

Which of the following is the BEST indicator of executive management's support for IT risk mitigation efforts?

- A. The number of stakeholders involved in IT risk identification workshops
- B. The percentage of corporate budget allocated to IT risk activities
- C. The percentage of incidents presented to the board
- D. The number of executives attending IT security awareness training

Answer: B

NEW QUESTION 38

- (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 43

- (Exam Topic 3)

Which of the following would be the GREATEST concern for an IT risk practitioner when an employees.....

- A. The organization's structure has not been updated
- B. Unnecessary access permissions have not been removed.
- C. Company equipment has not been retained by IT
- D. Job knowledge was not transferred to employees in the former department

Answer: B

NEW QUESTION 45

- (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 50

- (Exam Topic 3)

Which of the following will help ensure the effective decision-making of an IT risk management committee?

- A. Key stakeholders are enrolled as members
- B. Approved minutes are forwarded to senior management
- C. Committee meets at least quarterly
- D. Functional overlap across the business is minimized

Answer: D

NEW QUESTION 52

- (Exam Topic 3)

To communicate the risk associated with IT in business terms, which of the following MUST be defined?

- A. Compliance objectives
- B. Risk appetite of the organization
- C. Organizational objectives
- D. Inherent and residual risk

Answer: C

NEW QUESTION 53

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 58

- (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 60

- (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 65

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 69

- (Exam Topic 3)

Determining if organizational risk is tolerable requires:

- A. mapping residual risk with cost of controls
- B. comparing against regulatory requirements
- C. comparing industry risk appetite with the organization's.
- D. understanding the organization's risk appetite.

Answer: D

NEW QUESTION 74

- (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 77

- (Exam Topic 3)

The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP) system should be based on:

- A. stakeholder risk tolerance.
- B. benchmarking criteria.
- C. suppliers used by the organization.
- D. the control environment.

Answer: D

NEW QUESTION 78

- (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 82

- (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 83

- (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 87

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 88

- (Exam Topic 3)

Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?

- A. Vulnerability scanning
- B. Systems log correlation analysis
- C. Penetration testing
- D. Monitoring of intrusion detection system (IDS) alerts

Answer: C

NEW QUESTION 93

- (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 94

- (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 96

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 100

- (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 105

- (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 109

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 113

- (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 116

- (Exam Topic 3)

Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?

- A. The value at which control effectiveness would fail
- B. Thresholds benchmarked to peer organizations
- C. A typical operational value
- D. A value that represents the intended control state

Answer: A

NEW QUESTION 118

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 120

- (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 123

- (Exam Topic 3)

Which of the following would BEST enable a risk-based decision when considering the use of an emerging technology for data processing?

- A. Gap analysis
- B. Threat assessment
- C. Resource skills matrix
- D. Data quality assurance plan

Answer: A

NEW QUESTION 128

- (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 129

- (Exam Topic 3)

The BEST way to improve a risk register is to ensure the register:

- A. is updated based upon significant events.
- B. documents possible countermeasures.
- C. contains the risk assessment completion date.
- D. is regularly audited.

Answer: A

NEW QUESTION 133

- (Exam Topic 3)

What information is MOST helpful to asset owners when classifying organizational assets for risk assessment?

- A. Potential loss to tie business due to non-performance of the asset
- B. Known emerging environmental threats
- C. Known vulnerabilities published by the asset developer
- D. Cost of replacing the asset with a new asset providing similar services

Answer: A

NEW QUESTION 135

- (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 140

- (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 144

- (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 148

- (Exam Topic 3)

Which of the following BEST mitigates the risk of violating privacy laws when transferring personal information to a supplier?

- A. Encrypt the data while in transit to the supplier
- B. Contractually obligate the supplier to follow privacy laws.
- C. Require independent audits of the supplier's control environment
- D. Utilize blockchain during the data transfer

Answer: B

NEW QUESTION 151

- (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 152

- (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 156

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 159

- (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 163

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 167

- (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 169

- (Exam Topic 3)

A management team is on an aggressive mission to launch a new product to penetrate new markets and overlooks IT risk factors, threats, and vulnerabilities. This scenario BEST demonstrates an organization's risk:

- A. management.
- B. tolerance.
- C. culture.
- D. analysis.

Answer: C

NEW QUESTION 174

- (Exam Topic 3)

An organization learns of a new ransomware attack affecting organizations worldwide. Which of the following should be done FIRST to reduce the likelihood of infection from the attack?

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

Answer: A

NEW QUESTION 178

- (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 180

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 183

- (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 187

- (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 190

- (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 192

- (Exam Topic 3)

Which of the following facilitates a completely independent review of test results for evaluating control effectiveness?

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

Answer: B

NEW QUESTION 196

- (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 200

- (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 202

- (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 207

- (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 209

- (Exam Topic 3)

When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs?

- A. Risk management
- B. Change management
- C. Problem management
- D. Quality management

Answer: B

NEW QUESTION 210

- (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 212

- (Exam Topic 3)

Which of the following should be the risk practitioner's FIRST course of action when an organization plans to adopt a cloud computing strategy?

- A. Request a budget for implementation
- B. Conduct a threat analysis.
- C. Create a cloud computing policy.
- D. Perform a controls assessment.

Answer: B

NEW QUESTION 216

- (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 219

- (Exam Topic 3)

Which of the following scenarios represents a threat?

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

Answer: D

NEW QUESTION 221

- (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 224

- (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 226

- (Exam Topic 3)

Which of the following is MOST important to the effectiveness of key performance indicators (KPIs)?

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

Answer: A

NEW QUESTION 229

- (Exam Topic 3)

Which of the following findings of a security awareness program assessment would cause the GREATEST concern to a risk practitioner?

- A. The program has not decreased threat counts.
- B. The program has not considered business impact.
- C. The program has been significantly revised
- D. The program uses non-customized training modules.

Answer: D

NEW QUESTION 231

- (Exam Topic 3)

Which of the following contributes MOST to the effective implementation of risk responses?

- A. Clear understanding of the risk
- B. Comparable industry risk trends
- C. Appropriate resources
- D. Detailed standards and procedures

Answer: A

NEW QUESTION 234

- (Exam Topic 3)

An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?

- A. Management may be unable to accurately evaluate the risk profile.
- B. Resources may be inefficiently allocated.
- C. The same risk factor may be identified in multiple areas.
- D. Multiple risk treatment efforts may be initiated to treat a given risk.

Answer: B

NEW QUESTION 238

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 242

- (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 244

- (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 249

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 251

- (Exam Topic 3)

Which of the following is MOST likely to cause a key risk indicator (KRI) to exceed thresholds?

- A. Occurrences of specific events
- B. A performance measurement
- C. The risk tolerance level
- D. Risk scenarios

Answer: C

NEW QUESTION 255

- (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 259

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 261

- (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 266

- (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 269

- (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 273

- (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 278

- (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 279

- (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 281

- (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 285

- (Exam Topic 2)

The PRIMARY benefit of classifying information assets is that it helps to:

- A. communicate risk to senior management
- B. assign risk ownership
- C. facilitate internal audit
- D. determine the appropriate level of control

Answer: D

NEW QUESTION 290

- (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 293

- (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 294

- (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 296

- (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 298

- (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 302

- (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 307

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 308

- (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 310

- (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 312

- (Exam Topic 2)

When presenting risk, the BEST method to ensure that the risk is measurable against the organization's risk appetite is through the use of a:

- A. risk map
- B. cause-and-effect diagram
- C. maturity model
- D. technology strategy plan.

Answer: C

NEW QUESTION 314

- (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 318

- (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 322

- (Exam Topic 2)

Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?

- A. Risk tolerance
- B. Risk appetite
- C. Risk awareness
- D. Risk policy

Answer: B

NEW QUESTION 324

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 325

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 327

- (Exam Topic 2)

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

- A. The data is measurable.
- B. The data is calculated continuously.
- C. The data is relevant.
- D. The data is automatically produced.

Answer: C

NEW QUESTION 330

- (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 334

- (Exam Topic 2)

The risk associated with a high-risk vulnerability in an application is owned by the:

- A. security department.
- B. business unit
- C. vendor.
- D. IT department.

Answer: B

NEW QUESTION 336

- (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 339

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 342

- (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 343

- (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 346

- (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 351

- (Exam Topic 2)

The risk associated with inadvertent disclosure of database records from a public cloud service provider (CSP) would MOST effectively be reduced by:

- A. encrypting the data
- B. including a nondisclosure clause in the CSP contract
- C. assessing the data classification scheme
- D. reviewing CSP access privileges

Answer: A

NEW QUESTION 356

- (Exam Topic 2)

Which of the following is the BEST way to detect zero-day malware on an end user's workstation?

- A. An antivirus program
- B. Database activity monitoring
- C. Firewall log monitoring
- D. File integrity monitoring

Answer: C

NEW QUESTION 357

- (Exam Topic 2)

An organization is measuring the effectiveness of its change management program to reduce the number of unplanned production changes. Which of the following would be the BEST metric to determine if the program is performing as expected?

- A. Decrease in the time to move changes to production
- B. Ratio of emergency fixes to total changes
- C. Ratio of system changes to total changes
- D. Decrease in number of changes without a fallback plan

Answer: B

NEW QUESTION 362

- (Exam Topic 2)

A large organization needs to report risk at all levels for a new centralized visualization project to reduce cost and improve performance. Which of the following would MOST effectively represent the overall risk of the project to senior management?

- A. Aggregated key performance indicators (KPIs)
- B. Key risk indicators (KRIs)
- C. Centralized risk register
- D. Risk heat map

Answer: D

NEW QUESTION 364

- (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 365

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 367

- (Exam Topic 2)

Who should be responsible for implementing and maintaining security controls?

- A. End user
- B. Internal auditor
- C. Data owner
- D. Data custodian

Answer: C

NEW QUESTION 372

- (Exam Topic 2)

When communicating changes in the IT risk profile, which of the following should be included to BEST enable stakeholder decision making?

- A. List of recent incidents affecting industry peers
- B. Results of external attacks and related compensating controls
- C. Gaps between current and desired states of the control environment
- D. Review of leading IT risk management practices within the industry

Answer: C

NEW QUESTION 375

- (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 378

- (Exam Topic 2)

Which of the following would be MOST helpful to a risk owner when making risk-aware decisions?

- A. Risk exposure expressed in business terms
- B. Recommendations for risk response options
- C. Resource requirements for risk responses
- D. List of business areas affected by the risk

Answer: A

NEW QUESTION 381

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 383

- (Exam Topic 2)

Which of The following would offer the MOST insight with regard to an organization's risk culture?

- A. Risk management procedures
- B. Senior management interviews
- C. Benchmark analyses
- D. Risk management framework

Answer: B

NEW QUESTION 387

- (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 390

- (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 395

- (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 398

- (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 399

- (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 404

- (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 407

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 410

- (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 414

- (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 416

- (Exam Topic 2)

Which of the following provides The MOST useful information when determining a risk management program's maturity level?

- A. Risk assessment results
- B. A recently reviewed risk register
- C. Key performance indicators (KPIs)
- D. The organization's risk framework

Answer: A

NEW QUESTION 419

- (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 423

- (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 425

- (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 429

- (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 434

- (Exam Topic 2)

Which of the following is the BEST indication that an organization's risk management program has not reached the desired maturity level?

- A. Significant increases in risk mitigation budgets
- B. Large fluctuations in risk ratings between assessments
- C. A steady increase in the time to recover from incidents
- D. A large number of control exceptions

Answer: B

NEW QUESTION 438

- (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 442

- (Exam Topic 2)

Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?

- A. Establishing a risk management committee
- B. Updating the organization's risk register to reflect the new threat
- C. Communicating the results of the threat impact analysis
- D. Establishing metrics to assess the effectiveness of the responses

Answer: C

NEW QUESTION 445

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 449

- (Exam Topic 1)

The analysis of which of the following will BEST help validate whether suspicious network activity is malicious?

- A. Logs and system events
- B. Intrusion detection system (IDS) rules
- C. Vulnerability assessment reports
- D. Penetration test reports

Answer: B

NEW QUESTION 450

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 451

- (Exam Topic 3)

Which of the following would BEST mitigate the ongoing risk associated with operating system (OS) vulnerabilities?

- A. Temporarily mitigate the OS vulnerabilities
- B. Document and implement a patching process
- C. Evaluate permanent fixes such as patches and upgrades
- D. Identify the vulnerabilities and applicable OS patches

Answer: B

NEW QUESTION 455

- (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 458

- (Exam Topic 3)

After the implementation of internal of Things (IoT) devices, new risk scenarios were identified. What is the PRIMARY reason to report this information to risk owners?

- A. To reevaluate continued use to IoT devices
- B. To add new controls to mitigate the risk
- C. To recommend changes to the IoT policy
- D. To confirm the impact to the risk profile

Answer: D

NEW QUESTION 462

- (Exam Topic 3)

Which of the following is the BEST approach when a risk practitioner has been asked by a business unit manager for special consideration during a risk assessment of a system?

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

Answer: B

NEW QUESTION 466

- (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 467

- (Exam Topic 3)

Which of the following will BEST help to ensure the continued effectiveness of the IT risk management function within an organization experiencing high employee turnover?

- A. Well documented policies and procedures
- B. Risk and issue tracking
- C. An IT strategy committee
- D. Change and release management

Answer: B

NEW QUESTION 472

- (Exam Topic 3)

Which of the following should be the PRIMARY focus of an IT risk awareness program?

- A. Ensure compliance with the organization's internal policies
- B. Cultivate long-term behavioral change.
- C. Communicate IT risk policy to the participants.

D. Demonstrate regulatory compliance.

Answer: B

NEW QUESTION 476

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 480

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 482

- (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 485

- (Exam Topic 3)

Which of the following is MOST helpful to understand the consequences of an IT risk event?

- A. Fault tree analysis
- B. Historical trend analysis
- C. Root cause analysis
- D. Business impact analysis (BIA)

Answer: D

NEW QUESTION 487

- (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 488

- (Exam Topic 3)

Which of the following should be the MOST important consideration for senior management when developing a risk response strategy?

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

Answer: A

NEW QUESTION 491

- (Exam Topic 3)

Which of the following BEST enables risk-based decision making in support of a business continuity plan (BCP)?

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

Answer: A

NEW QUESTION 495

- (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 500

- (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 505

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 508

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 511

- (Exam Topic 2)

An IT risk practitioner is evaluating an organization's change management controls over the last six months. The GREATEST concern would be an increase in:

- A. rolled back changes below management's thresholds.
- B. change-related exceptions per month.
- C. the average implementation time for changes.
- D. number of user stories approved for implementation.

Answer: B

NEW QUESTION 514

- (Exam Topic 2)

Before implementing instant messaging within an organization using a public solution, which of the following should be in place to mitigate data leakage risk?

- A. A data extraction tool
- B. An access control list
- C. An intrusion detection system (IDS)
- D. An acceptable usage policy

Answer: D

NEW QUESTION 516

- (Exam Topic 2)

Which of the following is a KEY outcome of risk ownership?

- A. Risk responsibilities are addressed.
- B. Risk-related information is communicated.
- C. Risk-oriented tasks are defined.
- D. Business process risk is analyzed.

Answer: A

NEW QUESTION 518

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 520

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 525

- (Exam Topic 2)

Once a risk owner has decided to implement a control to mitigate risk, it is MOST important to develop:

- A. a process for measuring and reporting control performance.
- B. an alternate control design in case of failure of the identified control.
- C. a process for bypassing control procedures in case of exceptions.
- D. procedures to ensure the effectiveness of the control.

Answer: A

NEW QUESTION 529

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 532

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 533

- (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 535

- (Exam Topic 2)

An organization is considering adopting artificial intelligence (AI). Which of the following is the risk practitioner's MOST important course of action?

- A. Develop key risk indicators (KRIs).
- B. Ensure sufficient pre-implementation testing.
- C. Identify applicable risk scenarios.
- D. Identify the organization's critical data.

Answer: C

NEW QUESTION 540

- (Exam Topic 2)

A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration when establishing a contingency plan and an alternate processing site?

- A. The alternative site is a hot site with equipment ready to resume processing immediately.
- B. The contingency plan provides for backup media to be taken to the alternative site.
- C. The contingency plan for high priority applications does not involve a shared cold site.
- D. The alternative site does not reside on the same fault to matter how the distance apart.

Answer: B

NEW QUESTION 541

- (Exam Topic 2)

Reviewing which of the following provides the BEST indication of an organizations risk tolerance?

- A. Risk sharing strategy
- B. Risk transfer agreements
- C. Risk policies
- D. Risk assessments

Answer: D

NEW QUESTION 543

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 547

- (Exam Topic 2)

During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?

- A. Communicate the decision to the risk owner for approval
- B. Seek approval from the previous action plan manager.
- C. Identify an owner for the new control.
- D. Modify the action plan in the risk register.

Answer: A

NEW QUESTION 548

- (Exam Topic 2)

Which of the following BEST promotes commitment to controls?

- A. Assigning control ownership
- B. Assigning appropriate resources
- C. Assigning a quality control review
- D. Performing regular independent control reviews

Answer: A

NEW QUESTION 550

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 555

- (Exam Topic 2)

Which of the following is MOST important to ensure when continuously monitoring the performance of a client-facing application?

- A. Objectives are confirmed with the business owner
- B. Control owners approve control changes.
- C. End-user acceptance testing has been conducted
- D. Performance information in the log is encrypted

Answer: D

NEW QUESTION 556

- (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 558

- (Exam Topic 2)

Which of the following is a KEY responsibility of the second line of defense?

- A. Implementing control activities
- B. Monitoring control effectiveness
- C. Conducting control self-assessments
- D. Owning risk scenarios

Answer: B

NEW QUESTION 563

- (Exam Topic 1)

Which of the following should be the HIGHEST priority when developing a risk response?

- A. The risk response addresses the risk with a holistic view.
- B. The risk response is based on a cost-benefit analysis.
- C. The risk response is accounted for in the budget.
- D. The risk response aligns with the organization's risk appetite.

Answer: D

NEW QUESTION 567

- (Exam Topic 1)

Which of the following would be a risk practitioner's 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 572

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 577

- (Exam Topic 1)

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

- A. risk assessment methodology.
- B. risk appetite.
- C. capabilities

D. asset value.

Answer: B

NEW QUESTION 582

- (Exam Topic 1)

Which of the following would be the BEST recommendation if the level of risk in the IT risk profile has decreased and is now below management's risk appetite?

- A. Optimize the control environment.
- B. Realign risk appetite to the current risk level.
- C. Decrease the number of related risk scenarios.
- D. Reduce the risk management budget.

Answer: A

NEW QUESTION 586

- (Exam Topic 1)

Which of the following is the BEST approach to use when creating a comprehensive set of IT risk scenarios?

- A. Derive scenarios from IT risk policies and standards.
- B. Map scenarios to a recognized risk management framework.
- C. Gather scenarios from senior management.
- D. Benchmark scenarios against industry peers.

Answer: A

NEW QUESTION 587

- (Exam Topic 1)

Which of the following is the BEST method to identify unnecessary controls?

- A. Evaluating the impact of removing existing controls
- B. Evaluating existing controls against audit requirements
- C. Reviewing system functionalities associated with business processes
- D. Monitoring existing key risk indicators (KRIs)

Answer: A

NEW QUESTION 589

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 590

- (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 594

- (Exam Topic 1)

An organization has identified a risk exposure due to weak technical controls in a newly implemented HR system. The risk practitioner is documenting the risk in the risk register. The risk should be owned by the:

- A. chief risk officer.
- B. project manager.
- C. chief information officer.
- D. business process owner.

Answer: D

NEW QUESTION 599

- (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 603

- (Exam Topic 1)

In addition to the risk register, what should a risk practitioner review to develop an understanding of the organization's risk profile?

- A. The control catalog
- B. The asset profile
- C. Business objectives
- D. Key risk indicators (KRIs)

Answer: C

NEW QUESTION 608

- (Exam Topic 1)

Which of the following is MOST helpful to ensure effective security controls for a cloud service provider?

- A. A control self-assessment
- B. A third-party security assessment report
- C. Internal audit reports from the vendor
- D. Service level agreement monitoring

Answer: B

NEW QUESTION 611

- (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 616

- (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 621

- (Exam Topic 1)

Which of the following is the BEST indication of an improved risk-aware culture following the implementation of a security awareness training program for all employees?

- A. A reduction in the number of help desk calls
- B. An increase in the number of identified system flaws
- C. A reduction in the number of user access resets
- D. An increase in the number of incidents reported

Answer: B

NEW QUESTION 624

- (Exam Topic 1)

After undertaking a risk assessment of a production system, the MOST appropriate action is for the risk manager to:

- A. recommend a program that minimizes the concerns of that production system.
- B. inform the development team of the concerns, and together formulate risk reduction measures.
- C. inform the process owner of the concerns and propose measures to reduce them
- D. inform the IT manager of the concerns and propose measures to reduce them.

Answer: A

NEW QUESTION 629

- (Exam Topic 1)

Which of the following is the BEST metric to demonstrate the effectiveness of an organization's change management process?

- A. Increase in the frequency of changes
- B. Percent of unauthorized changes
- C. Increase in the number of emergency changes
- D. Average time to complete changes

Answer: B

NEW QUESTION 632

- (Exam Topic 1)

Which of the following would BEST ensure that identified risk scenarios are addressed?

- A. Reviewing the implementation of the risk response
- B. Creating a separate risk register for key business units
- C. Performing real-time monitoring of threats
- D. Performing regular risk control self-assessments

Answer: C

NEW QUESTION 635

- (Exam Topic 1)

When determining which control deficiencies are most significant, which of the following would provide the MOST useful information?

- A. Risk analysis results
- B. Exception handling policy
- C. Vulnerability assessment results
- D. Benchmarking assessments

Answer: C

NEW QUESTION 636

- (Exam Topic 1)

Which of the following is the MOST useful indicator to measure the efficiency of an identity and access management process?

- A. Number of tickets for provisioning new accounts
- B. Average time to provision user accounts
- C. Password reset volume per month
- D. Average account lockout time

Answer: C

NEW QUESTION 641

- (Exam Topic 1)

Which of the following is the GREATEST benefit of incorporating IT risk scenarios into the corporate risk register?

- A. Corporate incident escalation protocols are established.
- B. Exposure is integrated into the organization's risk profile.
- C. Risk appetite cascades to business unit management
- D. The organization-wide control budget is expanded.

Answer: B

NEW QUESTION 646

- (Exam Topic 1)

IT risk assessments can BEST be used by management:

- A. for compliance with laws and regulations
- B. as a basis for cost-benefit analysis.
- C. as input for decision-making
- D. to measure organizational success.

Answer: C

NEW QUESTION 651

- (Exam Topic 1)

A web-based service provider with a low risk appetite for system outages is reviewing its current risk profile for online security. Which of the following observations would be MOST relevant to escalate to senior management?

- A. An increase in attempted distributed denial of service (DDoS) attacks
- B. An increase in attempted website phishing attacks
- C. A decrease in achievement of service level agreements (SLAs)
- D. A decrease in remediated web security vulnerabilities

Answer: A

NEW QUESTION 652

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 656

- (Exam Topic 1)

Which of the following would be MOST helpful when estimating the likelihood of negative events?

- A. Business impact analysis
- B. Threat analysis
- C. Risk response analysis
- D. Cost-benefit analysis

Answer: B

NEW QUESTION 661

- (Exam Topic 1)

Which of the following is the MOST important element of a successful risk awareness training program?

- A. Customizing content for the audience
- B. Providing incentives to participants
- C. Mapping to a recognized standard
- D. Providing metrics for measurement

Answer: A

NEW QUESTION 665

- (Exam Topic 1)

During the risk assessment of an organization that processes credit cards, a number of existing controls have been found to be ineffective and do not meet industry standards. The overall control environment may still be effective if:

- A. compensating controls are in place.
- B. a control mitigation plan is in place.
- C. risk management is effective.
- D. residual risk is accepted.

Answer: A

NEW QUESTION 667

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 671

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 675

- (Exam Topic 1)

A risk assessment has identified that departments have installed their own WiFi access points on the enterprise network. Which of the following would be MOST important to include in a report to senior management?

- A. The network security policy
- B. Potential business impact

- C. The WiFi access point configuration
- D. Planned remediation actions

Answer: B

NEW QUESTION 680

- (Exam Topic 1)

The MAIN purpose of conducting a control self-assessment (CSA) is to:

- A. gain a better understanding of the control effectiveness in the organization
- B. gain a better understanding of the risk in the organization
- C. adjust the controls prior to an external audit
- D. reduce the dependency on external audits

Answer: A

NEW QUESTION 682

- (Exam Topic 1)

Calculation of the recovery time objective (RTO) is necessary to determine the:

- A. time required to restore files.
- B. point of synchronization
- C. priority of restoration.
- D. annual loss expectancy (ALE).

Answer: A

NEW QUESTION 685

- (Exam Topic 1)

It is MOST appropriate for changes to be promoted to production after they are:

- A. communicated to business management
- B. tested by business owners.
- C. approved by the business owner.
- D. initiated by business users.

Answer: C

NEW QUESTION 688

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CRISC Practice Exam Features:

- * CRISC Questions and Answers Updated Frequently
- * CRISC Practice Questions Verified by Expert Senior Certified Staff
- * CRISC Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CRISC Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CRISC Practice Test Here](#)