



Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1

- (Exam Topic 3)

Which of the following should be an element of the risk appetite of an organization?

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

Answer: B

NEW QUESTION 2

- (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 3

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 4

- (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 5

- (Exam Topic 3)

Which of the following is the MOST important topic to cover in a risk awareness training program for all staff?

- A. Internal and external information security incidents
- B. The risk department's roles and responsibilities
- C. Policy compliance requirements and exceptions process
- D. The organization's information security risk profile

Answer: C

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
		A disgruntled								
		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 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 8

- (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 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)

Reviewing historical risk events is MOST useful for which of the following processes within the risk management life cycle?

- A. Risk monitoring
- B. Risk mitigation
- C. Risk aggregation
- D. Risk assessment

Answer: D

NEW QUESTION 10

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 12

- (Exam Topic 3)

Several network user accounts were recently created without the required management approvals. Which of the following would be the risk practitioner's BEST recommendation to address this situation?

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

Answer: C

NEW QUESTION 13

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 17

- (Exam Topic 3)

Which of the following will BEST help to ensure key risk indicators (KRIs) provide value to risk owners?

- A. Ongoing training
- B. Timely notification
- C. Return on investment (ROI)
- D. Cost minimization

Answer: B

NEW QUESTION 20

- (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 22

- (Exam Topic 3)

It is MOST important that security controls for a new system be documented in:

- A. testing requirements
- B. the implementation plan.
- C. System requirements
- D. The security policy

Answer: C

NEW QUESTION 27

- (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 31

- (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 35

- (Exam Topic 3)

Which of the following is the BEST indicator of the effectiveness of IT risk management processes?

- A. Percentage of business users completing risk training
- B. Percentage of high-risk scenarios for which risk action plans have been developed
- C. Number of key risk indicators (KRIs) defined
- D. Time between when IT risk scenarios are identified and the enterprise's response

Answer: B

NEW QUESTION 40

- (Exam Topic 3)

Which of the following is MOST important to the integrity of a security log?

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

Answer: B

NEW QUESTION 43

- (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 45

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 48

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 49

- (Exam Topic 3)

Which of the following is MOST important when considering risk in an enterprise risk management (ERM) process?

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

Answer: B

NEW QUESTION 52

- (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 54

- (Exam Topic 3)

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

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

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

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

Answer: A

NEW QUESTION 55

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 59

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 64

- (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 65

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 67

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 68

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 70

- (Exam Topic 3)

A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?

- A. Obtain the risk owner's approval.
- B. Record the risk as accepted in the risk register.
- C. Inform senior management.
- D. update the risk response plan.

Answer: A

NEW QUESTION 73

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 77

- (Exam Topic 3)

What is the PRIMARY purpose of a business impact analysis (BIA)?

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

Answer: D

NEW QUESTION 79

- (Exam Topic 3)

A peer review of a risk assessment finds that a relevant threat community was not included. Mitigation of the risk will require substantial changes to a software application. Which of the following is the BEST course of action?

- A. Ask the business to make a budget request to remediate the problem.
- B. Build a business case to remediate the fix.
- C. Research the types of attacks the threat can present.
- D. Determine the impact of the missing threat.

Answer: D

NEW QUESTION 80

- (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 82

- (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 85

- (Exam Topic 3)

The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for.

- A. data logging and monitoring
- B. data mining and analytics
- C. data classification and labeling
- D. data retention and destruction

Answer: C

NEW QUESTION 89

- (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 94

- (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 97

- (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 99

- (Exam Topic 3)

The BEST reason to classify IT assets during a risk assessment is to determine the:

- A. priority in the risk register.
- B. business process owner.
- C. enterprise risk profile.
- D. appropriate level of protection.

Answer: D

NEW QUESTION 102

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 107

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 110

- (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 111

- (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 112

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 116

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 118

- (Exam Topic 3)

An organization has initiated a project to launch an IT-based service to customers and take advantage of being the first to market. Which of the following should be of GREATEST concern to senior management?

- A. More time has been allotted for testing.
- B. The project is likely to deliver the product late.
- C. A new project manager is handling the project.
- D. The cost of the project will exceed the allotted budget.

Answer: B

NEW QUESTION 121

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 125

- (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 126

- (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 128

- (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 131

- (Exam Topic 3)

Which of the following roles would be MOST helpful in providing a high-level view of risk related to customer data loss?

- A. Customer database manager
- B. Customer data custodian
- C. Data privacy officer
- D. Audit committee

Answer: B

NEW QUESTION 135

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 137

- (Exam Topic 3)

A risk practitioner observed Vial a high number of pokey exceptions were approved by senior management. Which of the following is the risk practitioner's BEST course of action to determine root cause?

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

Answer: C

NEW QUESTION 138

- (Exam Topic 3)

A risk practitioner is utilizing a risk heat map during a risk assessment. Risk events that are coded with the same color will have a similar:

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

Answer: B

NEW QUESTION 141

- (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 143

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 146

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 151

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 156

- (Exam Topic 3)

While reviewing the risk register, a risk practitioner notices that different business units have significant variances in inherent risk for the same risk scenario. Which of the following is the BEST course of action?

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

Answer: B

NEW QUESTION 159

- (Exam Topic 3)

Which of the following BEST indicates whether security awareness training is effective?

- A. User self-assessment
- B. User behavior after training
- C. Course evaluation
- D. Quality of training materials

Answer: B

NEW QUESTION 164

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 165

- (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 170

- (Exam Topic 3)

Which of the following is the MOST critical factor to consider when determining an organization's risk appetite?

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

Answer: D

NEW QUESTION 174

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 176

- (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 178

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 181

- (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 183

- (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 184

- (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 186

- (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 189

- (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 194

- (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 196

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 198

- (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 201

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 205

- (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 206

- (Exam Topic 3)

Which of the following would require updates to an organization's IT risk register?

- A. Discovery of an ineffectively designed key IT control
- B. Management review of key risk indicators (KRIs)
- C. Changes to the team responsible for maintaining the register
- D. Completion of the latest internal audit

Answer: A

NEW QUESTION 210

- (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 215

- (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 220

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 222

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 225

- (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 229

- (Exam Topic 3)

Which of the following provides the BEST evidence that a selected risk treatment plan is effective?

- A. Identifying key risk indicators (KRIs)
- B. Evaluating the return on investment (ROI)
- C. Evaluating the residual risk level
- D. Performing a cost-benefit analysis

Answer: C

NEW QUESTION 232

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 234

- (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 238

- (Exam Topic 3)

Which of the following is MOST important information to review when developing plans for using emerging technologies?

- A. Existing IT environment
- B. IT strategic plan
- C. Risk register
- D. Organizational strategic plan

Answer: D

NEW QUESTION 241

- (Exam Topic 3)

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

- A. Perform a gap analysis.
- B. Prioritize impact to the business units.
- C. Perform a risk assessment.
- D. Review the risk tolerance and appetite.

Answer: C

NEW QUESTION 243

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 248

- (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 249

- (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 250

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 251

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 255

- (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 257

- (Exam Topic 3)

Accountability for a particular risk is BEST represented in a:

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

Answer: D

NEW QUESTION 259

- (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 262

- (Exam Topic 3)

Which of the following represents a vulnerability?

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

Answer: C

NEW QUESTION 265

- (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 268

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 273

- (Exam Topic 3)

Which of the following is MOST important to compare against the corporate risk profile?

- A. Industry benchmarks
- B. Risk tolerance

- C. Risk appetite
- D. Regulatory compliance

Answer: D

NEW QUESTION 274

- (Exam Topic 3)

An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

- A. Implement database activity and capacity monitoring.
- B. Ensure the business is aware of the risk.
- C. Ensure the enterprise has a process to detect such situations.
- D. Consider providing additional system resources to this job.

Answer: C

NEW QUESTION 278

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 279

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 282

- (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 285

- (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 289

- (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 294

- (Exam Topic 3)

Which of the following BEST indicates the efficiency of a process for granting access privileges?

- A. Average time to grant access privileges
- B. Number of changes in access granted to users
- C. Average number of access privilege exceptions
- D. Number and type of locked obsolete accounts

Answer: C

NEW QUESTION 298

- (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 300

- (Exam Topic 3)

To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:

- A. require the vendor to sign a nondisclosure agreement
- B. clearly define the project scope.
- C. perform background checks on the vendor.
- D. notify network administrators before testing

Answer: A

NEW QUESTION 302

- (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 303

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 307

- (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 309

- (Exam Topic 3)

Which of The following is the MOST comprehensive input to the risk assessment process specific to the effects of system downtime?

- A. Business continuity plan (BCP) testing results
- B. Recovery lime objective (RTO)
- C. Business impact analysis (BIA)
- D. results Recovery point objective (RPO)

Answer: C

NEW QUESTION 310

- (Exam Topic 3)

The objective of aligning mitigating controls to risk appetite is to ensure that:

- A. exposures are reduced to the fullest extent
- B. exposures are reduced only for critical business systems
- C. insurance costs are minimized
- D. the cost of controls does not exceed the expected loss.

Answer: D

NEW QUESTION 313

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 317

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 318

- (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 321

- (Exam Topic 3)

An organization control environment is MOST effective when:

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

Answer: B

NEW QUESTION 322

- (Exam Topic 3)

Who is BEST suited to provide objective input when updating residual risk to reflect the results of control effectiveness?

- A. Control owner
- B. Risk owner
- C. Internal auditor
- D. Compliance manager

Answer: C

NEW QUESTION 326

- (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 329

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 334

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 339

- (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 344

- (Exam Topic 3)

After the review of a risk record, internal audit questioned why the risk was lowered from medium to low. Which of the following is the BEST course of action in responding to this inquiry?

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

Answer: B

NEW QUESTION 345

- (Exam Topic 3)

A risk practitioner has become aware of production data being used in a test environment. Which of the following should be the practitioner's PRIMARY concern?

- A. Sensitivity of the data
- B. Readability of test data
- C. Security of the test environment
- D. Availability of data to authorized staff

Answer: A

NEW QUESTION 348

- (Exam Topic 3)

A newly hired risk practitioner finds that the risk register has not been updated in the past year. What is the risk practitioner's BEST course of action?

- A. Identify changes in risk factors and initiate risk reviews.
- B. Engage an external consultant to redesign the risk management process.
- C. Outsource the process for updating the risk register.
- D. Implement a process improvement and replace the old risk register.

Answer: A

NEW QUESTION 350

- (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 354

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 357

- (Exam Topic 3)

Who should be accountable for monitoring the control environment to ensure controls are effective?

- A. Risk owner
- B. Security monitoring operations
- C. Impacted data owner
- D. System owner

Answer: A

NEW QUESTION 362

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 364

- (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 366

- (Exam Topic 3)

Which of the following is MOST helpful in preventing risk events from materializing?

- A. Prioritizing and tracking issues
- B. Establishing key risk indicators (KRIs)
- C. Reviewing and analyzing security incidents
- D. Maintaining the risk register

Answer: A

NEW QUESTION 368

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 369

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 370

- (Exam Topic 3)

Which of the following would BEST mitigate an identified risk scenario?

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

Answer: C

NEW QUESTION 371

- (Exam Topic 3)

A service provider is managing a client's servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider's MOST appropriate action would be to:

- A. develop a risk remediation plan overriding the client's decision
- B. make a note for this item in the next audit explaining the situation
- C. insist that the remediation occur for the benefit of other customers
- D. ask the client to document the formal risk acceptance for the provider

Answer: D

NEW QUESTION 372

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 375

- (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 379

- (Exam Topic 3)

Effective risk communication BEST benefits an organization by:

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

Answer: A

NEW QUESTION 382

- (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 386

- (Exam Topic 3)

For a large software development project, risk assessments are MOST effective when performed:

- A. before system development begins.
- B. at system development.
- C. at each stage of the system development life cycle (SDLC).
- D. during the development of the business case.

Answer: C

NEW QUESTION 388

- (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 389

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 393

- (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 395

- (Exam Topic 2)

An organization's internal audit department is considering the implementation of robotics process automation (RPA) to automate certain continuous auditing tasks. Who would own the risk associated with ineffective design of the software bots?

- A. Lead auditor
- B. Project manager
- C. Chief audit executive (CAE)
- D. Chief information officer (CIO)

Answer: C

NEW QUESTION 398

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 402

- (Exam Topic 2)

A recent internal risk review reveals the majority of core IT application recovery time objectives (RTOs) have exceeded the maximum time defined by the business application owners. Which of the following is MOST likely to change as a result?

- A. Risk forecasting
- B. Risk tolerance
- C. Risk likelihood
- D. Risk appetite

Answer: B

NEW QUESTION 406

- (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 410

- (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 415

- (Exam Topic 2)

Which of the following is the MOST important consideration when determining whether to accept residual risk after security controls have been implemented on a critical system?

- A. Cost versus benefit of additional mitigating controls
- B. Annualized loss expectancy (ALE) for the system
- C. Frequency of business impact
- D. Cost of the Information control system

Answer: A

NEW QUESTION 420

- (Exam Topic 2)

The annualized loss expectancy (ALE) method of risk analysis:

- A. helps in calculating the expected cost of controls
- B. uses qualitative risk rankings such as lo
- C. medium and high.
- D. can be used m a cost-benefit analysts
- E. can be used to determine the indirect business impact.

Answer: C

NEW QUESTION 425

- (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 430

- (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 435

- (Exam Topic 2)

The PRIMARY basis for selecting a security control is:

- A. to achieve the desired level of maturity.

- B. the materiality of the risk.
- C. the ability to mitigate risk.
- D. the cost of the control.

Answer: C

NEW QUESTION 439

- (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 441

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 443

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 447

- (Exam Topic 2)

Which of the following activities is PRIMARILY the responsibility of senior management?

- A. Bottom-up identification of emerging risks
- B. Categorization of risk scenarios against a standard taxonomy
- C. Prioritization of risk scenarios based on severity
- D. Review of external loss data

Answer: C

NEW QUESTION 452

- (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 453

- (Exam Topic 2)

A business manager wants to leverage an existing approved vendor solution from another area within the organization. Which of the following is the risk practitioner's BEST course of action?

- A. Recommend allowing the new usage based on prior approval.
- B. Request a new third-party review.
- C. Request revalidation of the original use case.
- D. Assess the risk associated with the new use case.

Answer: D

NEW QUESTION 456

- (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 459

- (Exam Topic 2)

Which of the following should be the PRIMARY focus of an independent review of a risk management process?

- A. Accuracy of risk tolerance levels
- B. Consistency of risk process results
- C. Participation of stakeholders
- D. Maturity of the process

Answer: B

NEW QUESTION 464

- (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 465

- (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 469

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 471

- (Exam Topic 2)

It is MOST important to the effectiveness of an IT risk management function that the associated processes are:

- A. aligned to an industry-accepted framework.
- B. reviewed and approved by senior management.
- C. periodically assessed against regulatory requirements.
- D. updated and monitored on a continuous basis.

Answer: C

NEW QUESTION 472

- (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 475

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 478

- (Exam Topic 2)

A risk practitioner notices that a particular key risk indicator (KRI) has remained below its established trigger point for an extended period of time. Which of the following should be done FIRST?

- A. Recommend a re-evaluation of the current threshold of the KRI.
- B. Notify management that KRIs are being effectively managed.
- C. Update the risk rating associated with the KRI in the risk register.
- D. Update the risk tolerance and risk appetite to better align to the KRI.

Answer: A

NEW QUESTION 483

- (Exam Topic 2)

A bank wants to send a critical payment order via email to one of its offshore branches. Which of the following is the BEST way to ensure the message reaches the intended recipient without alteration?

- A. Add a digital certificate
- B. Apply multi-factor authentication
- C. Add a hash to the message
- D. Add a secret key

Answer: C

NEW QUESTION 485

- (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 489

- (Exam Topic 2)

During the control evaluation phase of a risk assessment, it is noted that multiple controls are ineffective. Which of the following should be the risk practitioner's FIRST course of action?

- A. Recommend risk remediation of the ineffective controls.
- B. Compare the residual risk to the current risk appetite.
- C. Determine the root cause of the control failures.
- D. Escalate the control failures to senior management.

Answer: C

NEW QUESTION 490

- (Exam Topic 2)

When establishing leading indicators for the information security incident response process it is MOST important to consider the percentage of reported incidents:

- A. that result in a full root cause analysis.
- B. used for verification within the SLA.
- C. that are verified as actual incidents.
- D. resolved within the SLA.

Answer: C

NEW QUESTION 494

- (Exam Topic 2)

Performing a background check on a new employee candidate before hiring is an example of what type of control?

- A. Detective
- B. Compensating
- C. Corrective

D. Preventive

Answer: C

NEW QUESTION 499

- (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 502

- (Exam Topic 2)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?

- A. Percentage of vulnerabilities remediated within the agreed service level
- B. Number of vulnerabilities identified during the period
- C. Number of vulnerabilities re-opened during the period
- D. Percentage of vulnerabilities escalated to senior management

Answer: A

NEW QUESTION 507

- (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 512

- (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 513

- (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 514

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 515

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 520

- (Exam Topic 2)

The BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability remediation program is the number of:

- A. vulnerability scans.
- B. recurring vulnerabilities.
- C. vulnerabilities remediated,
- D. new vulnerabilities identified.

Answer: C

NEW QUESTION 521

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 524

- (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 525

- (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 527

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 530

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 533

- (Exam Topic 2)

During a risk assessment, the risk practitioner finds a new risk scenario without controls has been entered into the risk register. Which of the following is the MOST appropriate action?

- A. Include the new risk scenario in the current risk assessment.
- B. Postpone the risk assessment until controls are identified.
- C. Request the risk scenario be removed from the register.
- D. Exclude the new risk scenario from the current risk assessment

Answer: A

NEW QUESTION 534

- (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 539

- (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 544

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 545

- (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 547

- (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 550

- (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 552

- (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 556

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 557

- (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 562

- (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 563

- (Exam Topic 2)

A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (PII). Which of the following will MOST likely outcome for an organization affected by the new law?

- A. Increase in compliance breaches
- B. Increase in loss event impact
- C. Increase in residual risk
- D. Increase in customer complaints

Answer: B

NEW QUESTION 567

- (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 568

- (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 569

- (Exam Topic 2)

Which of the following is MOST helpful in identifying gaps between the current and desired state of the IT risk environment?

- A. Analyzing risk appetite and tolerance levels
- B. Assessing identified risk and recording results in the risk register
- C. Evaluating risk scenarios and assessing current controls
- D. Reviewing guidance from industry best practices and standards

Answer: C

NEW QUESTION 574

- (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 576

- (Exam Topic 2)

A business unit has decided to accept the risk of implementing an off-the-shelf, commercial software package that uses weak password controls. The BEST course of action would be to:

- A. obtain management approval for policy exception.
- B. develop an improved password software routine.
- C. select another application with strong password controls.
- D. continue the implementation with no changes.

Answer: B

NEW QUESTION 578

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 583

- (Exam Topic 2)

Which stakeholders are PRIMARILY responsible for determining enterprise IT risk appetite?

- A. Audit and compliance management
- B. The chief information officer (CIO) and the chief financial officer (CFO)
- C. Enterprise risk management and business process owners
- D. Executive management and the board of directors

Answer: D

NEW QUESTION 587

- (Exam Topic 2)

A risk practitioner shares the results of a vulnerability assessment for a critical business application with the business manager. Which of the following is the NEXT step?

- A. Develop a risk action plan to address the findings.
- B. Evaluate the impact of the vulnerabilities to the business application.
- C. Escalate the findings to senior management and internal audit.
- D. Conduct a penetration test to validate the vulnerabilities from the findings.

Answer: B

NEW QUESTION 592

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 595

- (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 597

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 598

- (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 601

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 603

- (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 604

- (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 606

- (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 609

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 614

- (Exam Topic 2)

What is the GREATEST concern with maintaining decentralized risk registers instead of a consolidated risk register?

- A. Aggregated risk may exceed the enterprise's risk appetite and tolerance.
- B. Duplicate resources may be used to manage risk registers.
- C. Standardization of risk management practices may be difficult to enforce.
- D. Risk analysis may be inconsistent due to non-uniform impact and likelihood scales.

Answer: C

NEW QUESTION 616

- (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 621

- (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 624

- (Exam Topic 2)

Which of the following would BEST help identify the owner for each risk scenario in a risk register?

- A. Determining which departments contribute most to risk
- B. Allocating responsibility for risk factors equally to asset owners
- C. Mapping identified risk factors to specific business processes
- D. Determining resource dependency of assets

Answer: C

NEW QUESTION 629

- (Exam Topic 2)

Which of the following is MOST important to understand when developing key risk indicators (KRIs)?

- A. KRI thresholds
- B. Integrity of the source data
- C. Control environment
- D. Stakeholder requirements

Answer: B

NEW QUESTION 631

- (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 632

- (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 635

- (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 639

- (Exam Topic 2)

What should be the PRIMARY objective for a risk practitioner performing a post-implementation review of an IT risk mitigation project?

- A. Documenting project lessons learned
- B. Validating the risk mitigation project has been completed
- C. Confirming that the project budget was not exceeded
- D. Verifying that the risk level has been lowered

Answer: A

NEW QUESTION 644

- (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 645

- (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 648

- (Exam Topic 2)

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

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

Answer:

D

NEW QUESTION 653

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 657

- (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 662

- (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 667

- (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 668

- (Exam Topic 2)

The MOST important reason to monitor key risk indicators (KRIs) is to help management:

- A. identify early risk transfer strategies.
- B. lessen the impact of realized risk.
- C. analyze the chain of risk events.
- D. identify the root cause of risk events.

Answer: C

NEW QUESTION 671

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 674

- (Exam Topic 2)

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

- A. Change management as determined by a change control board
- B. Benchmarking analysis with similar completed projects

- C. Project governance criteria as determined by the project office
- D. The risk owner as determined by risk management processes

Answer: D

NEW QUESTION 679

- (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 681

- (Exam Topic 2)

The PRIMARY objective of The board of directors periodically reviewing the risk profile is to help ensure:

- A. the risk strategy is appropriate
- B. KRIs and KPIs are aligned
- C. performance of controls is adequate
- D. the risk monitoring process has been established

Answer: A

NEW QUESTION 684

- (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 687

- (Exam Topic 2)

Which of the following is the GREATEST risk associated with the use of data analytics?

- A. Distributed data sources
- B. Manual data extraction
- C. Incorrect data selection
- D. Excessive data volume

Answer: C

NEW QUESTION 692

- (Exam Topic 1)

Which of the following is the PRIMARY factor in determining a recovery time objective (RTO)?

- A. Cost of offsite backup premises
- B. Cost of downtime due to a disaster
- C. Cost of testing the business continuity plan
- D. Response time of the emergency action plan

Answer: B

NEW QUESTION 695

- (Exam Topic 1)

Which of the following elements of a risk register is MOST likely to change as a result of change in management's risk appetite?

- A. Key risk indicator (KRI) thresholds
- B. Inherent risk
- C. Risk likelihood and impact
- D. Risk velocity

Answer: A

NEW QUESTION 699

- (Exam Topic 1)

An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?

- A. Invoke the disaster recovery plan during an incident.
- B. Prepare a cost-benefit analysis of alternatives available
- C. Implement redundant infrastructure for the application.
- D. Reduce the recovery time by strengthening the response team.

Answer: C

NEW QUESTION 701

- (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 706

- (Exam Topic 3)

Which of the following should be the GREATEST concern for an organization that uses open source software applications?

- A. Lack of organizational policy regarding open source software
- B. Lack of reliability associated with the use of open source software
- C. Lack of monitoring over installation of open source software in the organization
- D. Lack of professional support for open source software

Answer: A

NEW QUESTION 711

- (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 714

- (Exam Topic 3)

Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

- A. Ability to determine business impact
- B. Up-to-date knowledge on risk responses
- C. Decision-making authority for risk treatment
- D. Awareness of emerging business threats

Answer: A

NEW QUESTION 716

- (Exam Topic 3)

The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:

- A. changes due to emergencies.
- B. changes that cause incidents.
- C. changes not requiring user acceptance testing.
- D. personnel that have rights to make changes in production.

Answer: B

NEW QUESTION 717

- (Exam Topic 3)

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

- A. Implement segregation of duties.
- B. Enforce an internal data access policy.
- C. Enforce the use of digital signatures.
- D. Apply single sign-on for access control.

Answer: B

NEW QUESTION 721

- (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 722

- (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 724

- (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 727

- (Exam Topic 3)

A change management process has recently been updated with new testing procedures. What is the NEXT course of action?

- A. Monitor processes to ensure recent updates are being followed.
- B. Communicate to those who test and promote changes.
- C. Conduct a cost-benefit analysis to justify the cost of the control.
- D. Assess the maturity of the change management process.

Answer: A

NEW QUESTION 729

- (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 734

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 736

- (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 741

- (Exam Topic 3)

A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?

- A. Develop a mechanism for monitoring residual risk.
- B. Update the risk register with the results.
- C. Prepare a business case for the response options.
- D. Identify resources for implementing responses.

Answer: C

NEW QUESTION 743

- (Exam Topic 3)

Which of the following would be a risk practitioner's BEST recommendation upon learning of an updated cybersecurity regulation that could impact the organization?

- A. Perform a gap analysis
- B. Conduct system testing
- C. Implement compensating controls
- D. Update security policies

Answer: A

NEW QUESTION 744

- (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 749

- (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 754

- (Exam Topic 3)

Which of the following is the MOST important consideration for protecting data assets in a Business application system?

- A. Application controls are aligned with data classification rules
- B. Application users are periodically trained on proper data handling practices
- C. Encrypted communication is established between applications and data servers
- D. Offsite encrypted backups are automatically created by the application

Answer: A

NEW QUESTION 756

- (Exam Topic 3)

The MAIN purpose of reviewing a control after implementation is to validate that the control:

- A. operates as intended.
- B. is being monitored.
- C. meets regulatory requirements.
- D. operates efficiently.

Answer: A

NEW QUESTION 760

- (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 762

- (Exam Topic 3)

The PRIMARY objective of collecting information and reviewing documentation when performing periodic risk analysis should be to:

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

Answer: D

NEW QUESTION 764

- (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 768

- (Exam Topic 3)

When reviewing a report on the performance of control processes, it is MOST important to verify whether the:

- A. business process objectives have been met.
- B. control adheres to regulatory standards.
- C. residual risk objectives have been achieved.
- D. control process is designed effectively.

Answer: D

NEW QUESTION 769

- (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 771

- (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 776

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 779

- (Exam Topic 3)

Which of the following is the GREATEST benefit of identifying appropriate risk owners?

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

Answer: A

NEW QUESTION 783

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 784

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 785

- (Exam Topic 3)

Which of the following is the BEST approach to mitigate the risk associated with a control deficiency?

- A. Perform a business case analysis
- B. Implement compensating controls.
- C. Conduct a control self-assessment (CSA)
- D. Build a provision for risk

Answer: C

NEW QUESTION 787

- (Exam Topic 3)

A recent vulnerability assessment of a web-facing application revealed several weaknesses. Which of the following should be done NEXT to determine the risk exposure?

- A. Code review
- B. Penetration test
- C. Gap assessment
- D. Business impact analysis (BIA)

Answer: B

NEW QUESTION 790

- (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 791

- (Exam Topic 2)

An organization is making significant changes to an application. At what point should the application risk profile be updated?

- A. After user acceptance testing (UAT)
- B. Upon release to production
- C. During backlog scheduling
- D. When reviewing functional requirements

Answer: D

NEW QUESTION 794

- (Exam Topic 2)

Which of the following is the BEST way to determine software license compliance?

- A. List non-compliant systems in the risk register.
- B. Conduct periodic compliance reviews.
- C. Review whistleblower reports of noncompliance.
- D. Monitor user software download activity.

Answer: B

NEW QUESTION 795

- (Exam Topic 2)

A risk assessment indicates the residual risk associated with a new bring your own device (BYOD) program is within organizational risk tolerance. Which of the following should the risk practitioner recommend be done NEXT?

- A. Implement targeted awareness training for new BYOD users.
- B. Implement monitoring to detect control deterioration.
- C. Identify log sources to monitor BYOD usage and risk impact.
- D. Reduce the risk tolerance level.

Answer: B

NEW QUESTION 798

- (Exam Topic 2)

A maturity model will BEST indicate:

- A. confidentiality and integrity.
- B. effectiveness and efficiency.
- C. availability and reliability.
- D. certification and accreditation.

Answer: B

NEW QUESTION 799

- (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 802

- (Exam Topic 2)

Which of the following would be of GREATEST assistance when justifying investment in risk response strategies?

- A. Total cost of ownership
- B. Resource dependency analysis
- C. Cost-benefit analysis
- D. Business impact analysis

Answer: C

NEW QUESTION 807

- (Exam Topic 2)

Which of the following should be the PRIMARY recipient of reports showing the progress of a current IT risk mitigation project?

- A. Senior management
- B. Project manager
- C. Project sponsor
- D. IT risk manager

Answer: A

NEW QUESTION 810

- (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 813

- (Exam Topic 2)

Which of the following should be a risk practitioner's MOST important consideration when developing IT risk scenarios?

- A. The impact of controls on the efficiency of the business in delivering services
- B. Linkage of identified risk scenarios with enterprise risk management
- C. Potential threats and vulnerabilities that may have an impact on the business
- D. Results of network vulnerability scanning and penetration testing

Answer: C

NEW QUESTION 818

- (Exam Topic 2)

An external security audit has reported multiple findings related to control noncompliance. Which of the following would be MOST important for the risk practitioner to communicate to senior management?

- A. A recommendation for internal audit validation
- B. Plans for mitigating the associated risk
- C. Suggestions for improving risk awareness training
- D. The impact to the organization's risk profile

Answer: D

NEW QUESTION 819

- (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 824

- (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 826

- (Exam Topic 2)

A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:

- A. strategy.
- B. profile.
- C. process.
- D. map.

Answer: A

NEW QUESTION 829

- (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 833

- (Exam Topic 2)

An organization has raised the risk appetite for technology risk. The MOST likely result would be:

- A. increased inherent risk.
- B. higher risk management cost
- C. decreased residual risk.

D. lower risk management cost.

Answer: D

NEW QUESTION 835

- (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 837

- (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 840

- (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 841

- (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 844

- (Exam Topic 2)

Implementing which of the following will BEST help ensure that systems comply with an established baseline before deployment?

- A. Vulnerability scanning
- B. Continuous monitoring and alerting
- C. Configuration management
- D. Access controls and active logging

Answer: C

NEW QUESTION 848

- (Exam Topic 2)

Which of the following would be the GREATEST concern related to data privacy when implementing an Internet of Things (IoT) solution that collects personally identifiable information (PII)?

- A. A privacy impact assessment has not been completed.
- B. Data encryption methods apply to a subset of PII obtained.
- C. The data privacy officer was not consulted.
- D. Insufficient access controls are used on the IoT devices.

Answer: A

NEW QUESTION 850

- (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 852

- (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 856

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 861

- (Exam Topic 2)

Which of the following is the GREATEST concern associated with the transmission of healthcare data across the internet?

- A. Unencrypted data
- B. Lack of redundant circuits
- C. Low bandwidth connections
- D. Data integrity

Answer: A

NEW QUESTION 865

- (Exam Topic 2)

Who should be responsible for strategic decisions on risk management?

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

Answer: B

NEW QUESTION 869

- (Exam Topic 2)

Which of the following provides the BEST evidence that risk mitigation plans have been implemented effectively?

- A. Self-assessments by process owners
- B. Mitigation plan progress reports
- C. Risk owner attestation
- D. Change in the level of residual risk

Answer: D

NEW QUESTION 870

- (Exam Topic 2)

A large organization is replacing its enterprise resource planning (ERP) system and has decided not to deploy the payroll module of the new system. Instead, the current payroll system will continue to be used. Of the following, who should own the risk if the ERP and payroll system fail to operate as expected?

- A. The business owner
- B. The ERP administrator
- C. The project steering committee
- D. The IT project manager

Answer: A

NEW QUESTION 873

- (Exam Topic 1)

Which of the following risk register updates is MOST important for senior management to review?

- A. Extending the date of a future action plan by two months
- B. Retiring a risk scenario no longer used
- C. Avoiding a risk that was previously accepted
- D. Changing a risk owner

Answer: A

NEW QUESTION 875

.....

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](#)