

## Exam Questions CRISC

Certified in Risk and Information Systems Control

<https://www.2passeasy.com/dumps/CRISC/>



#### NEW QUESTION 1

- (Exam Topic 3)

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

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

**Answer: B**

#### NEW QUESTION 2

- (Exam Topic 3)

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

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

**Answer: C**

#### NEW QUESTION 3

- (Exam Topic 3)

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

- A. Demonstration that the control is operating as designed
- B. A successful walk-through of the associated risk assessment
- C. Management attestation that the control is operating effectively
- D. Automated data indicating that risk has been reduced

**Answer: C**

#### NEW QUESTION 4

- (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 5

- (Exam Topic 3)

Which of the following would MOST likely cause a risk practitioner to change the likelihood rating in the risk register?

- A. Risk appetite
- B. Control cost
- C. Control effectiveness
- D. Risk tolerance

**Answer: C**

#### NEW QUESTION 6

- (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 7

- (Exam Topic 3)

Which of the following is MOST important when conducting a post-implementation review as part of the system development life cycle (SDLC)?

- A. Verifying that project objectives are met
- B. Identifying project cost overruns
- C. Leveraging an independent review team
- D. Reviewing the project initiation risk matrix

**Answer:** A

**NEW QUESTION 8**

- (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 9**

- (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 10**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 10**

- (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 12**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 13**

- (Exam Topic 3)

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

- A. An established process for project change management
- B. Retention of test data and results for review purposes
- C. Business managements review of functional requirements
- D. Segregation between development, test, and production

**Answer:** A

**NEW QUESTION 15**

- (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 16

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 17

- (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 22

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 27

- (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 31

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 33

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 38

- (Exam Topic 3)

Which of the following would provide the MOST useful information to a risk owner when reviewing the progress of risk mitigation?

- A. Key audit findings
- B. Treatment plan status
- C. Performance indicators
- D. Risk scenario results

**Answer:** C

#### NEW QUESTION 43

- (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 46

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 50

- (Exam Topic 3)

Vulnerabilities have been detected on an organization's systems. Applications installed on these systems will not operate if the underlying servers are updated.

Which of the following is the risk practitioner's BEST course of action?

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

**Answer:** D

#### NEW QUESTION 53

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 57

- (Exam Topic 3)

A bank recently incorporated Blockchain technology with the potential to impact known risk within the organization. Which of the following is the risk practitioner's BEST course of action?

- A. Determine whether risk responses are still adequate.
- B. Analyze and update control assessments with the new processes.
- C. Analyze the risk and update the risk register as needed.
- D. Conduct testing of the control that mitigate the existing risk.

**Answer:** B

#### NEW QUESTION 62

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 67**

- (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 71**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 74**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 75**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 77**

- (Exam Topic 3)

Which of the following is MOST helpful to mitigate the risk associated with an application under development not meeting business objectives?

- A. Identifying tweets that may compromise enterprise architecture (EA)
- B. Including diverse Business scenarios in user acceptance testing (UAT)
- C. Performing risk assessments during the business case development stage
- D. Including key stakeholders in review of user requirements

**Answer:** D

**NEW QUESTION 82**

- (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 83**

- (Exam Topic 3)

An IT control gap has been identified in a key process. Who would be the MOST appropriate owner of the risk associated with this gap?

- A. Key control owner
- B. Operational risk manager



- C. Business process owner
- D. Chief information security officer (CISO)

**Answer:** A

#### NEW QUESTION 84

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 85

- (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 87

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 89

- (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 92

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 95

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 97

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 102

- (Exam Topic 3)

Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

- A. Key performance indicators (KPIs)
- B. Risk heat maps
- C. Internal audit findings
- D. Periodic penetration testing

**Answer:** A

#### NEW QUESTION 104

- (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 106

- (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 108

- (Exam Topic 3)

Which of the following is the BEST indication that key risk indicators (KRIs) should be revised?

- A. A decrease in the number of critical assets covered by risk thresholds
- B. An Increase In the number of risk threshold exceptions
- C. An increase in the number of change events pending management review
- D. A decrease In the number of key performance indicators (KPIs)

**Answer:** B

#### NEW QUESTION 112

- (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 114

- (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 119

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 120

- (Exam Topic 3)

Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

- A. Aligning IT with short-term and long-term goals of the organization
- B. Ensuring the IT budget and resources focus on risk management
- C. Ensuring senior management's primary focus is on the impact of identified risk
- D. Prioritizing internal departments that provide service to customers

**Answer:** A

#### NEW QUESTION 121

- (Exam Topic 3)

Which of the following would be MOST helpful when communicating roles associated with the IT risk management process?

- A. Skills matrix
- B. Job descriptions
- C. RACI chart
- D. Organizational chart

**Answer:** C

#### NEW QUESTION 125

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 127

- (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 129

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 130

- (Exam Topic 3)

Which of the following tasks should be completed prior to creating a disaster recovery plan (DRP)?

- A. Conducting a business impact analysis (BIA)
- B. Identifying the recovery response team
- C. Procuring a recovery site
- D. Assigning sensitivity levels to data

**Answer:** A

**NEW QUESTION 131**

- (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 132**

- (Exam Topic 3)

A risk practitioner has been asked by executives to explain how existing risk treatment plans would affect risk posture at the end of the year. Which of the following is MOST helpful in responding to this request?

- A. Assessing risk with no controls in place
- B. Showing projected residual risk
- C. Providing peer benchmarking results
- D. Assessing risk with current controls in place

**Answer:** D

**NEW QUESTION 134**

- (Exam Topic 3)

The BEST key performance indicator (KPI) to measure the effectiveness of a backup process would be the number of:

- A. resources to monitor backups
- B. restoration monitoring reports
- C. backup recovery requests
- D. recurring restore failures

**Answer:** D

**NEW QUESTION 139**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 143**

- (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 147**

- (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 148**

- (Exam Topic 3)

The PRIMARY objective of a risk identification process is to:

- A. evaluate how risk conditions are managed.
- B. determine threats and vulnerabilities.

- C. estimate anticipated financial impact of risk conditions.
- D. establish risk response options.

**Answer:** B

#### NEW QUESTION 152

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 155

- (Exam Topic 3)

An organization automatically approves exceptions to security policies on a recurring basis. This practice is MOST likely the result of:

- A. a lack of mitigating actions for identified risk
- B. decreased threat levels
- C. ineffective service delivery
- D. ineffective IT governance

**Answer:** D

#### NEW QUESTION 158

- (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 163

- (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 165

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 169

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 172

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 174

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 178

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 181

- (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 186

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 190

- (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 194

- (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 195

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 197

- (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 201

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 203

- (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 204

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 209

- (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 213

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 217**

- (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 221**

- (Exam Topic 3)

Legal and regulatory risk associated with business conducted over the Internet is driven by:

- A. the jurisdiction in which an organization has its principal headquarters
- B. international law and a uniform set of regulations.
- C. the laws and regulations of each individual country
- D. international standard-setting bodies.

**Answer:** C

**NEW QUESTION 224**

- (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 228**

- (Exam Topic 3)

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

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

**Answer:** D

**NEW QUESTION 233**

- (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 236**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 241**

- (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 242

- (Exam Topic 3)

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

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

**Answer:** A

#### NEW QUESTION 243

- (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 247

- (Exam Topic 3)

A violation of segregation of duties is when the same:

- A. user requests and tests the change prior to production.
- B. user authorizes and monitors the change post-implementation.
- C. programmer requests and tests the change prior to production.
- D. programmer writes and promotes code into production.

**Answer:** D

#### NEW QUESTION 252

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 256

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 260

- (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 264

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 266**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 268**

- (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 270**

- (Exam Topic 3)

Which of the following provides the BEST measurement of an organization's risk management maturity level?

- A. Level of residual risk
- B. The results of a gap analysis
- C. IT alignment to business objectives
- D. Key risk indicators (KRIs)

**Answer:** C

**NEW QUESTION 272**

- (Exam Topic 3)

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

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

**Answer:** B

**NEW QUESTION 273**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 277**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 278**

- (Exam Topic 2)

The MAIN purpose of a risk register is to:

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

**Answer:** C

#### NEW QUESTION 282

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 285

- (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 290

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 291

- (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 293

- (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 298

- (Exam Topic 2)

A bank has outsourced its statement printing function to an external service provider. Which of the following is the MOST critical requirement to include in the contract?

- A. Monitoring of service costs
- B. Provision of internal audit reports
- C. Notification of sub-contracting arrangements
- D. Confidentiality of customer data

**Answer:** D

#### NEW QUESTION 301

- (Exam Topic 2)

Which of the following is MOST helpful in verifying that the implementation of a risk mitigation control has been completed as intended?

- A. An updated risk register
- B. Risk assessment results
- C. Technical control validation
- D. Control testing results

**Answer:** D

#### NEW QUESTION 306

- (Exam Topic 2)

A risk practitioner has been notified that an employee sent an email in error containing customers' personally identifiable information (PII). Which of the following is the risk practitioner's BEST course of action?

- A. Report it to the chief risk officer.
- B. Advise the employee to forward the email to the phishing team.
- C. follow incident reporting procedures.
- D. Advise the employee to permanently delete the email.

**Answer:** C

#### NEW QUESTION 309

- (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 312

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 317

- (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 320

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 322

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 323**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 327**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 330**

- (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 333**

- (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 338**

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 341**

- (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 346**

- (Exam Topic 2)

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

- A. Key risk indicators (KRIs)
- B. Data backups

- C. Incident response plan
- D. Cyber insurance

**Answer:** C

#### NEW QUESTION 348

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 349

- (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 352

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 354

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 355

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 357

- (Exam Topic 2)

Prior to selecting key performance indicators (KPIs), it is MOST important to ensure:

- A. trending data is available.
- B. process flowcharts are current.
- C. measurement objectives are defined.
- D. data collection technology is available.

**Answer:** C

#### NEW QUESTION 362

- (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 365

- (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 367

- (Exam Topic 2)

Implementing which of the following controls would BEST reduce the impact of a vulnerability that has been exploited?

- A. Detective control
- B. Deterrent control
- C. Preventive control
- D. Corrective control

**Answer:** D

#### NEW QUESTION 370

- (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 374

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 375

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 378

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 380

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 384

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 388

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 392

- (Exam Topic 2)

Which of the following is the PRIMARY reason to update a risk register with risk assessment results?

- A. To communicate the level and priority of assessed risk to management
- B. To provide a comprehensive inventory of risk across the organization
- C. To assign a risk owner to manage the risk
- D. To enable the creation of action plans to address risk

**Answer: A**

#### NEW QUESTION 396

- (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 399

- (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 401

- (Exam Topic 2)

A risk practitioner has just learned about new data FIRST?

- A. Notify executive management.
- B. Analyze the impact to the organization.
- C. Update the IT risk register.
- D. Design IT risk mitigation plans.

**Answer: B**

#### NEW QUESTION 405

- (Exam Topic 2)

Which of the following BEST indicates that an organizations risk management program is effective?

- A. Fewer security incidents have been reported.
- B. The number of audit findings has decreased.
- C. Residual risk is reduced.
- D. inherent risk is unchanged.

**Answer:** C

#### NEW QUESTION 407

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 412

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 417

- (Exam Topic 2)

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

- A. Reviewing access control lists
- B. Authorizing user access requests
- C. Performing user access recertification
- D. Terminating inactive user access

**Answer:** B

#### NEW QUESTION 422

- (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 424

- (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 429

- (Exam Topic 2)

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

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

**Answer:** B

**NEW QUESTION 432**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 434**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 435**

- (Exam Topic 2)

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

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

**Answer:** C

**NEW QUESTION 440**

- (Exam Topic 2)

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

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

**Answer:** D

**NEW QUESTION 443**

- (Exam Topic 2)

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

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

**Answer:** A

**NEW QUESTION 445**

- (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 449**

- (Exam Topic 2)

What are the MOST important criteria to consider when developing a data classification scheme to facilitate risk assessment and the prioritization of risk mitigation

activities?

- A. Mitigation and control value
- B. Volume and scope of data generated daily
- C. Business criticality and sensitivity
- D. Recovery point objective (RPO) and recovery time objective (RTO)

**Answer:** C

#### NEW QUESTION 451

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 452

- (Exam Topic 2)

Who is PRIMARILY accountable for risk treatment decisions?

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

**Answer:** A

#### NEW QUESTION 453

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 454

- (Exam Topic 2)

The PRIMARY reason for periodically monitoring key risk indicators (KRIs) is to:

- A. rectify errors in results of KRIs.
- B. detect changes in the risk profile.
- C. reduce costs of risk mitigation controls.
- D. continually improve risk assessments.

**Answer:** B

#### NEW QUESTION 458

- (Exam Topic 2)

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

- A. Results of current and past risk assessments
- B. Organizational strategy and objectives
- C. Lessons learned from materialized risk scenarios
- D. Internal and external audit findings

**Answer:** B

#### NEW QUESTION 459

- (Exam Topic 2)

The GREATEST concern when maintaining a risk register is that:

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

**Answer:** D

#### NEW QUESTION 460

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 461

- (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 465

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 467

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 469

- (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 474

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 477

- (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 479

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 483

- (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 488

- (Exam Topic 3)

Which of the following is MOST important to include in a risk assessment of an emerging technology?

- A. Risk response plans
- B. Risk and control ownership
- C. Key controls
- D. Impact and likelihood ratings

**Answer:** D

#### NEW QUESTION 490

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 491

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 493

- (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 496

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 497**

- (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 499**

- (Exam Topic 3)

An organization is planning to move its application infrastructure from on-premises to the cloud. Which of the following is the BEST course of the action to address the risk associated with data transfer if the relationship is terminated with the vendor?

- A. Meet with the business leaders to ensure the classification of their transferred data is in place
- B. Ensure the language in the contract explicitly states who is accountable for each step of the data transfer process
- C. Collect requirements for the environment to ensure the infrastructure as a service (IaaS) is configured appropriately.
- D. Work closely with the information security officer to ensure the company has the proper security controls in place.

**Answer:** B

**NEW QUESTION 504**

- (Exam Topic 3)

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

- A. Alignment with regulatory requirements
- B. Availability of qualitative data
- C. Properly set thresholds
- D. Alignment with industry benchmarks

**Answer:** C

**NEW QUESTION 508**

- (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 509**

- (Exam Topic 3)

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

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

**Answer:** C

**NEW QUESTION 511**

- (Exam Topic 3)

The PRIMARY reason for prioritizing risk scenarios is to:

- A. provide an enterprise-wide view of risk
- B. support risk response tracking
- C. assign risk ownership
- D. facilitate risk response decisions.

**Answer:** D

**NEW QUESTION 515**

- (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 519

- (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 522

- (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 524

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 528

- (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 530

- (Exam Topic 3)

Risk acceptance of an exception to a security control would MOST likely be justified when:

- A. automation cannot be applied to the control
- B. business benefits exceed the loss exposure.
- C. the end-user license agreement has expired.
- D. the control is difficult to enforce in practice.

**Answer:** B

#### NEW QUESTION 533

- (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 536

- (Exam Topic 2)

An identified high probability risk scenario involving a critical, proprietary business function has an annualized cost of control higher than the annual loss

expectancy. Which of the following is the BEST risk response?

- A. Mitigate
- B. Accept
- C. Transfer
- D. Avoid

**Answer:** B

#### NEW QUESTION 539

- (Exam Topic 2)

The MOST effective approach to prioritize risk scenarios is by:

- A. assessing impact to the strategic plan.
- B. aligning with industry best practices.
- C. soliciting input from risk management experts.
- D. evaluating the cost of risk response.

**Answer:** A

#### NEW QUESTION 540

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 545

- (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 549

- (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 551

- (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 554

- (Exam Topic 2)

The risk appetite for an organization could be derived from which of the following?

- A. Cost of controls
- B. Annual loss expectancy (ALE)
- C. Inherent risk
- D. Residual risk

**Answer:** A

#### NEW QUESTION 558

- (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 560

- (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 565

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 569

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 574

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 579

- (Exam Topic 2)

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

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

**Answer:** C

#### NEW QUESTION 584

- (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 588

- (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 593

- (Exam Topic 1)

A risk practitioner has identified that the organization's secondary data center does not provide redundancy for a critical application. Who should have the authority to accept the associated risk?

- A. Business continuity director
- B. Disaster recovery manager
- C. Business application owner
- D. Data center manager

**Answer: C**

#### NEW QUESTION 598

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 602

- (Exam Topic 1)

The BEST way to justify the risk mitigation actions recommended in a risk assessment would be to:

- A. align with audit results.
- B. benchmark with competitor s actions.
- C. reference best practice.
- D. focus on the business drivers

**Answer: D**

#### NEW QUESTION 605

- (Exam Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 609

- (Exam Topic 1)

A risk practitioners PRIMARY focus when validating a risk response action plan should be that risk response:

- A. reduces risk to an acceptable level
- B. quantifies risk impact
- C. aligns with business strategy
- D. advances business objectives.

**Answer: A**

#### NEW QUESTION 611

- (Exam Topic 1)

Which of the following is MOST critical when designing controls?

- A. Involvement of internal audit
- B. Involvement of process owner
- C. Quantitative impact of the risk



D. Identification of key risk indicators

**Answer: B**

#### NEW QUESTION 614

- (Exam Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 618

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 622

- (Exam Topic 1)

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

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

**Answer: A**

#### NEW QUESTION 626

- (Exam Topic 1)

A risk practitioner is summarizing the results of a high-profile risk assessment sponsored by senior management. The BEST way to support risk-based decisions by senior management would be to:

- A. map findings to objectives.
- B. provide a quantified detailed analysts.
- C. recommend risk tolerance thresholds.
- D. quantify key risk indicators (KRIs).

**Answer: A**

#### NEW QUESTION 628

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 630

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 631

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 633

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 638

- (Exam Topic 1)

Risk management strategies are PRIMARILY adopted to:

- A. take necessary precautions for claims and losses.
- B. achieve acceptable residual risk levels.
- C. avoid risk for business and IT assets.
- D. achieve compliance with legal requirements.

**Answer:** B

#### NEW QUESTION 640

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 642

- (Exam Topic 1)

Management has noticed storage costs have increased exponentially over the last 10 years because most users do not delete their emails. Which of the following can BEST alleviate this issue while not sacrificing security?

- A. Implementing record retention tools and techniques
- B. Establishing e-discovery and data loss prevention (DLP)
- C. Sending notifications when near storage quota
- D. Implementing a bring your own device (BYOD) policy

**Answer:** A

#### NEW QUESTION 643

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 645

- (Exam Topic 1)

In an organization with a mature risk management program, which of the following would provide the BEST evidence that the IT risk profile is up to date?

- A. Risk questionnaire
- B. Risk register
- C. Management assertion
- D. Compliance manual

**Answer:** B

#### NEW QUESTION 648

- (Exam Topic 1)

Which of the following should be the risk practitioner's PRIMARY focus when determining whether controls are adequate to mitigate risk?

- A. Sensitivity analysis
- B. Level of residual risk
- C. Cost-benefit analysis
- D. Risk appetite

**Answer: C**

#### NEW QUESTION 649

- (Exam Topic 1)

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

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

**Answer: D**

#### NEW QUESTION 654

- (Exam Topic 1)

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

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

**Answer: C**

#### NEW QUESTION 659

- (Exam Topic 1)

Which of the following is the MOST important data source for monitoring key risk indicators (KRIs)?

- A. Directives from legal and regulatory authorities
- B. Audit reports from internal information systems audits
- C. Automated logs collected from different systems
- D. Trend analysis of external risk factors

**Answer: C**

#### NEW QUESTION 661

- (Exam Topic 1)

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

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

**Answer: B**

#### NEW QUESTION 664

- (Exam Topic 1)

An organization has procured a managed hosting service and just discovered the location is likely to be flooded every 20 years. Of the following, who should be notified of this new information FIRST.

- A. The risk owner who also owns the business service enabled by this infrastructure
- B. The data center manager who is also employed under the managed hosting services contract
- C. The site manager who is required to provide annual risk assessments under the contract
- D. The chief information officer (CIO) who is responsible for the hosted services

**Answer: A**

#### NEW QUESTION 667

- (Exam Topic 1)

An organization has allowed its cyber risk insurance to lapse while seeking a new insurance provider. The risk practitioner should report to management that the risk has been:

- A. transferred
- B. mitigated.
- C. accepted
- D. avoided

Answer: C

**NEW QUESTION 670**

- (Exam Topic 1)

An effective control environment is BEST indicated by controls that:

- A. minimize senior management's risk tolerance.
- B. manage risk within the organization's risk appetite.
- C. reduce the thresholds of key risk indicators (KRIs).
- D. are cost-effective to implement

Answer: B

**NEW QUESTION 675**

- (Exam Topic 1)

A contract associated with a cloud service provider MUST include:

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

Answer: A

**NEW QUESTION 678**

- (Exam Topic 1)

An organization wants to assess the maturity of its internal control environment. The FIRST step should be to:

- A. validate control process execution.
- B. determine if controls are effective.
- C. identify key process owners.
- D. conduct a baseline assessment.

Answer: C

**NEW QUESTION 679**

- (Exam Topic 1)

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

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

Answer: D

**NEW QUESTION 684**

- (Exam Topic 1)

A risk practitioner is organizing a training session to communicate risk assessment methodologies to ensure a consistent risk view within the organization Which of the following is the MOST important topic to cover in this training?

- A. Applying risk appetite
- B. Applying risk factors
- C. Referencing risk event data
- D. Understanding risk culture

Answer: D

**NEW QUESTION 688**

- (Exam Topic 1)

The PRIMARY reason a risk practitioner would be interested in an internal audit report is to:

- A. plan awareness programs for business managers.
- B. evaluate maturity of the risk management process.
- C. assist in the development of a risk profile.
- D. maintain a risk register based on noncompliances.

Answer: C

**NEW QUESTION 689**

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CRISC Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CRISC Product From:

<https://www.2passeasy.com/dumps/CRISC/>

## Money Back Guarantee

### 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 FirstTry
- \* CRISC Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year