

Isaca

CRISC



Web: www.dumpscollection.com

Email: support@dumpscollection.com

Version: 14.0

[Total Questions: 674]



IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@dumpscollection.com

Support

If you have any questions about our product, please provide the following items:

- o exam code
- screenshot of the question
- login id/email

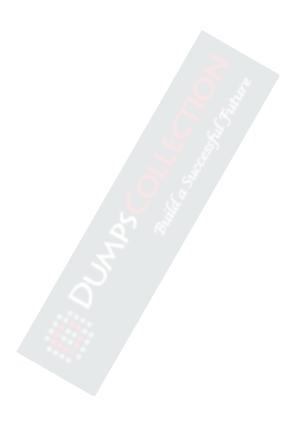
please contact us at support@dumpscollection.com and our technical experts will provide support within 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently. Any unauthorized changes will inflict legal punishment. We reserve the right of final explanation for this statement.

Exam Topic Breakdown

Exam Topic	Number of Questions
Topic 1 : Pool A	208
Topic 2 : Pool B	466
TOTAL	674



Topic 1, Pool A

Question #:1 - (Exam Topic 1)

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

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

Answer: C

Question #:2 - (Exam Topic 1)

The head of a business operations department asks to review the entire IT risk register. Which of the following would be the risk manager s BEST approach to this request before sharing the register?

- A. Escalate to senior management
- B. Require a nondisclosure agreement.
- C. Sanitize portions of the register
- D. Determine the purpose of the request

Answer: D

Question #:3 - (Exam Topic 1)

The PRIMARY objective for selecting risk response options is to:

- A. reduce risk 10 an acceptable level.
- B. identify compensating controls.
- C. minimize residual risk.
- D. reduce risk factors.

Answer: A

Question #:4 - (Exam Topic 1)

Who should be accountable for ensuring effective cybersecurity controls are established?

- A. Risk owner
- B. Security management function
- C. IT management
- D. Enterprise risk function

Answer: B

Question #:5 - (Exam Topic 1)

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

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

Answer: B

Question #:6 - (Exam Topic 1)

The number of tickets to rework application code has significantly exceeded the established threshold. Which of the following would be the risk practitioner's BEST recommendation?

- A. Perform a root cause analysis
- B. Perform a code review
- C. Implement version control software.
- D. Implement training on coding best practices

Answer: A

Question #:7 - (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

Question #:8 - (Exam Topic 1)

Which of the following IT controls is MOST useful in mitigating the risk associated with inaccurate data?

- A. Encrypted storage of data
- B. Links to source data
- C. Audit trails for updates and deletions
- D. Check totals on data records and data fields

Answer: C

Question #:9 - (Exam Topic 1)

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

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

Answer: B

Question #:10 - (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

Question #:11 - (Exam Topic 1)

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

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

Answer: B

Question #:12 - (Exam Topic 1)

Which of the following is the FIRST step in managing the security risk associated with wearable technology in the workplace?

- A. Identify the potential risk.
- B. Monitor employee usage.
- C. Assess the potential risk.
- D. Develop risk awareness training.

Answer: A

Question #:13 - (Exam Topic 1)

Which of the following is a PRIMARY benefit of engaging the risk owner during the risk assessment process?

- A. Identification of controls gaps that may lead to noncompliance
- B. Prioritization of risk action plans across departments
- C. Early detection of emerging threats

D. Accurate measurement of loss impact

Answer: D

Question #:14 - (Exam Topic 1)

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

Question #:15 - (Exam Topic 1)

Which of the following is the MOST important characteristic of an effective risk management program?

- A. Risk response plans are documented
- B. Controls are mapped to key risk scenarios.
- C. Key risk indicators are defined.
- D. Risk ownership is assigned

Answer: D

Question #:16 - (Exam Topic 1)

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

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

Answer: A

Question #:17 - (Exam Topic 1)

A trusted third party service provider has determined that the risk of a client's systems being hacked is low. Which of the following would be the client's BEST course of action?

- A. Perform their own risk assessment
- B. Implement additional controls to address the risk.
- C. Accept the risk based on the third party's risk assessment
- D. Perform an independent audit of the third party.

Answer: C

Question #:18 - (Exam Topic 1)

Which of the following is the MOST effective key performance indicator (KPI) for change management?

- A. Percentage of changes with a fallback plan
- B. Number of changes implemented
- C. Percentage of successful changes
- D. Average time required to implement a change

Answer: C

Question #:19 - (Exam Topic 1)

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

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

Answer: C

Question #:20 - (Exam Topic 1)

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

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

Answer: A

Question #:21 - (Exam Topic 1)

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: A

Question #:22 - (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

Question #:23 - (Exam Topic 1)

An organization has outsourced its IT security operations to a third party. Who is ULTIMATELY accountable for the risk associated with the outsourced operations?

- A. The third party s management
- B. The organization's management
- C. The control operators at the third party

D. The organization's vendor management office

Answer: B

Question #:24 - (Exam Topic 1)

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: A

Question #:25 - (Exam Topic 1)

Which of the following should be the PRIMARY consideration when implementing controls for monitoring user activity logs?

- A. Ensuring availability of resources for log analysis
- B. Implementing log analysis tools to automate controls
- C. Ensuring the control is proportional to the risk
- D. Building correlations between logs collected from different sources

Answer: C

Question #:26 - (Exam Topic 1)

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

Question #:27 - (Exam Topic 1)

Which of the following would be the BEST way to help ensure the effectiveness of a data loss prevention (DLP) control that has been implemented to prevent the loss of credit card data?

- A. Testing the transmission of credit card numbers
- B. Reviewing logs for unauthorized data transfers
- C. Configuring the DLP control to block credit card numbers
- D. Testing the DLP rule change control process

Answer: A

Question #:28 - (Exam Topic 1)

Which of the following is the MOST important consideration when developing an organization's risk taxonomy?

- A. Leading industry frameworks
- B. Business context
- C. Regulatory requirements
- D. IT strategy

Answer: C

Question #:29 - (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

Question #:30 - (Exam Topic 1)

A risk assessment has identified that an organization may not be in compliance with industry regulations. The BEST course of action would be to:

- A. conduct a gap analysis against compliance criteria.
- B. identify necessary controls to ensure compliance.
- C. modify internal assurance activities to include control validation.
- D. collaborate with management to meet compliance requirements.

Answer: A

Question #:31 - (Exam Topic 1)

Which of the following is the MOST important factor affecting risk management in an organization?

- A. The risk manager's expertise
- B. Regulatory requirements
- C. Board of directors' expertise
- D. The organization's culture

Answer: B

Question #:32 - (Exam Topic 1)

An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?

- A. Sufficient resources are not assigned to IT development projects.
- B. Customer support help desk staff does not have adequate training.
- C. Email infrastructure does not have proper rollback plans.
- D. The corporate email system does not identify and store phishing emails.

Answer: A

Question #:33 - (Exam Topic 1)

Which of the following is the MAIN reason for documenting the performance of controls?

- A. Obtaining management sign-off
- B. Demonstrating effective risk mitigation
- C. Justifying return on investment
- D. Providing accurate risk reporting

Answer: D

Question #:34 - (Exam Topic 1)

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

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

Answer: C

Question #:35 - (Exam Topic 1)

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: D

Question #:36 - (Exam Topic 1)

While reviewing a contract of a cloud services vendor, it was discovered that the vendor refuses to accept liability for a sensitive data breach. Which of the following controls will BES reduce the risk associated with such a data breach?

A. Ensuring the vendor does not know the encryption key

- B. Engaging a third party to validate operational controls
- C. Using the same cloud vendor as a competitor
- D. Using field-level encryption with a vendor supplied key

Answer: A

Question #:37 - (Exam Topic 1)

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

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

Answer: D

Question #:38 - (Exam Topic 1)

Which of the following techniques would be used during a risk assessment to demonstrate to stakeholders that all known alternatives were evaluated?

- A. Control chart
- B. Sensitivity analysis
- C. Trend analysis
- D. Decision tree

Answer: D

Question #:39 - (Exam Topic 1)

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

- A. Report the gap to senior management
- B. Consult with the IT department to update the RTO

- C. Complete a risk exception form.
- D. Consult with the business owner to update the BCP

Answer: A

Question #:40 - (Exam Topic 1)

Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?

- A. Percentage of unpatched IT assets
- B. Percentage of IT assets without ownership
- C. The number of IT assets securely disposed during the past year
- D. The number of IT assets procured during the previous month

Answer: B

Question #:41 - (Exam Topic 1)

Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?

- A. Key risk indicators
- B. Risk scenarios
- C. Business impact analysis
- D. Threat analysis

Answer: B

Question #:42 - (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

Question #:43 - (Exam Topic 1)

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

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

Answer: D

Question #:44 - (Exam Topic 1)

Which of the following is the MOST common concern associated with outsourcing to a service provider?

- A. Lack of technical expertise
- B. Combining incompatible duties
- C. Unauthorized data usage
- D. Denial of service attacks

Answer: B

Question #:45 - (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

Question #:46 - (Exam Topic 1)

Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?

- A. Relevance to the business process
- B. Regulatory compliance requirements
- C. Cost-benefit analysis
- D. Comparison against best practice

Answer: B

Question #:47 - (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 1BVOD) policy

Answer: A

Question #:48 - (Exam Topic 1)

Which of the following would BEST help minimize the risk associated with social engineering threats?

- A. Enforcing employees sanctions
- B. Conducting phishing exercises
- C. Enforcing segregation of dunes
- D. Reviewing the organization's risk appetite

Answer: B

Question #:49 - (Exam Topic 1)

Which of the following is the PRIMARY reason for a risk practitioner to use global standards related to risk management?

- A. To build an organizational risk-aware culture
- B. To continuously improve risk management processes
- C. To comply with legal and regulatory requirements
- D. To identify gaps in risk management practices

Answer: B

Question #:50 - (Exam Topic 1)

Which of the following will BEST mitigate the risk associated with IT and business misalignment?

- A. Establishing business key performance indicators (KPIs)
- B. Introducing an established framework for IT architecture
- C. Establishing key risk indicators (KRIs)
- D. Involving the business process owner in IT strategy

Answer: D

Question #:51 - (Exam Topic 1)

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

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

Answer: B

Question #:52 - (Exam Topic 1)

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

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

Answer: A

Question #:53 - (Exam Topic 1)

Which of the following is MOST important to understand when determining an appropriate risk assessment approach?

- A. Complexity of the IT infrastructure
- B. Value of information assets
- C. Management culture
- D. Threats and vulnerabilities

Answer: A

Question #:54 - (Exam Topic 1)

Which of the following aspects of an IT risk and control self-assessment would be MOST important to include in a report to senior management?

- A. Changes in control design
- B. A decrease in the number of key controls
- C. Changes in control ownership
- D. An increase in residual risk

Answer: D

Question #:55 - (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

Question #:56 - (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

Question #:57 - (Exam Topic 1)

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

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

Answer: D

Question #:58 - (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

Question #:59 - (Exam Topic 1)

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

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

Answer: B

Question #:60 - (Exam Topic 1)

Which of the following would be considered a vulnerability?

- A. Delayed removal of employee access
- B. Authorized administrative access to HR files
- C. Corruption of files due to malware
- D. Server downtime due to a denial of service (DoS) attack

Answer: A

Question #:61 - (Exam Topic 1)

Improvements in the design and implementation of a control will MOST likely result in an update to:

- A. inherent risk.
- B. residual risk.
- C. risk appetite
- D. risk tolerance

Answer: B

Question #:62 - (Exam Topic 1)

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

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

Answer: A

Question #:63 - (Exam Topic 1)

Which of the following is of GREATEST concern when uncontrolled changes are made to the control environment?

- A. A decrease in control layering effectiveness
- B. An increase in inherent risk
- C. An increase in control vulnerabilities
- D. An increase in the level of residual risk

Answer: D

Question #:64 - (Exam Topic 1)

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

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

Answer: C

Question #:65 - (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: A

Question #:66 - (Exam Topic 1)

From a business perspective, which of the following is the MOST important objective of a disaster recovery test?

- A. The organization gains assurance it can recover from a disaster
- B. Errors are discovered in the disaster recovery process.
- C. All business critical systems are successfully tested.
- D. All critical data is recovered within recovery time objectives (RTOs).

Answer: B

Question #:67 - (Exam Topic 1)

Which of the following is MOST helpful in identifying new risk exposures due to changes in the business environment?

- A. Standard operating procedures
- B. SWOT analysis
- C. Industry benchmarking
- D. Control gap analysis

Answer: B

Question #:68 - (Exam Topic 1)

Which of the following is the MOST important consideration for a risk practitioner when making a system implementation go-live recommendation?

- A. Completeness of system documentation
- B. Results of end user acceptance testing

- C. Variances between planned and actual cost
- D. availability of in-house resources

Answer: B

Question #:69 - (Exam Topic 1)

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

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

Answer: A

Question #:70 - (Exam Topic 1)

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

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

Answer: B

Question #:71 - (Exam Topic 1)

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

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

D. assessment

Answer: C

Question #:72 - (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

Question #:73 - (Exam Topic 1)

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

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

Answer: B

Question #:74 - (Exam Topic 1)

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

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

Answer: C

Question #:75 - (Exam Topic 1)

Which of the following would be MOST useful when measuring the progress of a risk response action plan?

- A. Percentage of mitigated risk scenarios
- B. Annual loss expectancy (ALE) changes
- C. Resource expenditure against budget
- D. An up-to-date risk register

Answer: D

Question #:76 - (Exam Topic 1)

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

Question #:77 - (Exam Topic 1)

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 m the risk register.
- C. Inform senior management.
- D. update the risk response plan.

Answer: A

Question #:78 - (Exam Topic 1)

Which of the following tools is MOST effective in identifying trends in the IT risk profile?

- A. Risk self-assessment
- B. Risk register
- C. Risk dashboard
- D. Risk map

Answer: C

Question #:79 - (Exam Topic 1)

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

- A. The network security policy
- B. Potential business impact
- C. The WiFi access point configuration
- D. Planned remediation actions

Answer: B

Question #:80 - (Exam Topic 1)

Which of the following would provide the BEST guidance when selecting an appropriate risk treatment plan?

- A. Risk mitigation budget
- B. Business Impact analysis
- C. Cost-benefit analysis
- D. Return on investment

Answer: B

Question #:81 - (Exam Topic 1)

Which of the following is the PRIMARY reason to perform ongoing risk assessments?

- A. Emerging risk must be continuously reported to management.
- B. New system vulnerabilities emerge at frequent intervals.
- C. The risk environment is subject to change.

D. The information security budget must be justified.

Answer: C

Question #:82 - (Exam Topic 1)

A key risk indicator (KRI) is reported to senior management on a periodic basis as exceeding thresholds, but each time senior management has decided to take no action to reduce the risk. Which of the following is the MOST likely reason for senior management's response?

- A. The underlying data source for the KRI is using inaccurate data and needs to be corrected.
- B. The KRI is not providing useful information and should be removed from the KRI inventory.
- C. The KRI threshold needs to be revised to better align with the organization s risk appetite
- D. Senior management does not understand the KRI and should undergo risk training.

Answer: C

Question #:83 - (Exam Topic 1)

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

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

Answer: D

Question #:84 - (Exam Topic 1)

A PRIMARY advantage of involving business management in evaluating and managing risk is that management:

- A. better understands the system architecture.
- B. is more objective than risk management.
- C. can balance technical and business risk.
- D. can make better-informed business decisions.

Answer: D

Question #:85 - (Exam Topic 1)

A review of an organization s controls has determined its data loss prevention {DLP} system is currently failing to detect outgoing emails containing credit card data. Which of the following would be MOST impacted?

- A. Key risk indicators (KRls)
- B. Inherent risk
- C. Residual risk
- D. Risk appetite

Answer: C

Question #:86 - (Exam Topic 1)

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

- A. Updating the risk register to include the risk mitigation plan
- B. Determining processes for monitoring the effectiveness of the controls
- C. Ensuring that control design reduces risk to an acceptable level
- D. Confirming to management the controls reduce the likelihood of the risk

Answer: A

Question #:87 - (Exam Topic 1)

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

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

Answer: A

Question #:88 - (Exam Topic 1)

Which of the following is MOST important when developing key performance indicators (KPIs)?

- A. Alignment to risk responses
- B. Alignment to management reports
- C. Alerts when risk thresholds are reached
- D. Identification of trends

Answer: C

Question #:89 - (Exam Topic 1)

Which of the following should be the PRIMARY objective of promoting a risk-aware culture within an organization?

- A. Better understanding of the risk appetite
- B. Improving audit results
- C. Enabling risk-based decision making
- D. Increasing process control efficiencies

Answer: C

Question #:90 - (Exam Topic 1)

Which of the following would BEST help an enterprise prioritize risk scenarios?

- A. Industry best practices
- B. Placement on the risk map
- C. Degree of variances in the risk
- D. Cost of risk mitigation

Answer: B

Question #:91 - (Exam Topic 1)

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

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

Answer: B

Question #:92 - (Exam Topic 1)

Which of the following is MOST effective against external threats to an organizations confidential information?

- A. Single sign-on
- B. Data integrity checking
- C. Strong authentication
- D. Intrusion detection system

Answer: C

Ouestion #:93 - (Exam Topic 1)

When reviewing management's IT control self-assessments, a risk practitioner noted an ineffective control that links to several low residual risk scenarios. What should be the NEXT course of action?

- A. Assess management's risk tolerance.
- B. Recommend management accept the low risk scenarios.
- C. Propose mitigating controls
- D. Re-evaluate the risk scenarios associated with the control

Answer: D

Question #:94 - (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

Question #:95 - (Exam Topic 1)

Which of the following would be MOST important for a risk practitioner to provide to the internal audit department during the audit planning process?

- A. Closed management action plans from the previous audit
- B. Annual risk assessment results
- C. An updated vulnerability management report
- D. A list of identified generic risk scenarios

Answer: A

Question #:96 - (Exam Topic 1)

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:

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 7	The Scope The	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	Regulator

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

Answer: B

Question #:97 - (Exam Topic 1)

Which of the following is the MOST important consideration when multiple risk practitioners capture risk scenarios in a single risk register?

- A. Aligning risk ownership and control ownership
- B. Developing risk escalation and reporting procedures
- C. Maintaining up-to-date risk treatment plans
- D. Using a consistent method for risk assessment

Answer: D

Question #:98 - (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

Question #:99 - (Exam Topic 1)

Which of the following would BEST provide early warning of a high-risk condition?

- A. Risk register
- B. Risk assessment
- C. Key risk indicator (KRI)
- D. Key performance indicator (KPI)

Answer: C

Question #:100 - (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

Question #:101 - (Exam Topic 1)

Which of the following would MOST effectively enable a business operations manager to identify events exceeding risk thresholds?

- A. Continuous monitoring
- B. A control self-assessment
- C. Transaction logging
- D. Benchmarking against peers

Answer: A

Question #:102 - (Exam Topic 1)

A rule-based data loss prevention {DLP} tool has recently been implemented to reduce the risk of sensitive data leakage Which of the following is MOST likely to change as a result of this implementation?

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

Answer: A

Question #:103 - (Exam Topic 1)

Which of the following would BEST help to ensure that identified risk is efficiently managed?

A. Reviewing the maturity of the control environment

- B. Regularly monitoring the project plan
- C. Maintaining a key risk indicator for each asset in the risk register
- D. Periodically reviewing controls per the risk treatment plan

Answer: D

Question #:104 - (Exam Topic 1)

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

- A. risk assessment methodology.
- B. risk appetite.
- C. capabilities
- D. asset value.

Answer: B

Question #:105 - (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 (KRls)

Answer: C

Question #:106 - (Exam Topic 1)

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

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

Answer: C

Question #:107 - (Exam Topic 1)

During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall. Which of the following controls has MOST likely been compromised?

- A. Data validation
- B. Identification
- C. Authentication
- D. Data integrity

Answer: C

Question #:108 - (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

Question #:109 - (Exam Topic 1)

Which of the following is the BEST indication of an effective risk management program?

- A. Risk action plans are approved by senior management.
- B. Residual risk is within the organizational risk appetite
- C. Mitigating controls are designed and implemented.
- D. Risk is recorded and tracked in the risk register

Answer: B

Question #:110 - (Exam Topic 1)

Which of the following is the MOST important key performance indicator (KPI) to establish in the service level agreement (SLA) for an outsourced data center?

- A. Percentage of systems included in recovery processes
- B. Number of key systems hosted
- C. Average response time to resolve system incidents
- D. Percentage of system availability

Answer: C

Question #:111 - (Exam Topic 1)

Which of the following is the MOST important benefit of key risk indicators (KRIs)'

- A. Assisting in continually optimizing risk governance
- B. Enabling the documentation and analysis of trends
- C. Ensuring compliance with regulatory requirements
- D. Providing an early warning to take proactive actions

Answer: D

Question #:112 - (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

Question #:113 - (Exam Topic 1)

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

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

Answer: B

Question #:114 - (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

Question #:115 - (Exam Topic 1)

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

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

Answer: B

Question #:116 - (Exam Topic 1)

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 (KRls) 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

Question #:117 - (Exam Topic 1)

Which of the following BEST describes the role of the IT risk profile in strategic IT-related decisions?

- A. It compares performance levels of IT assets to value delivered.
- B. It facilitates the alignment of strategic IT objectives to business objectives.
- C. It provides input to business managers when preparing a business case for new IT projects.
- D. It helps assess the effects of IT decisions on risk exposure

Answer: D

Question #:118 - (Exam Topic 1)

What is the BEST information to present to business control owners when justifying costs related to controls?

- A. Loss event frequency and magnitude
- B. The previous year's budget and actuals
- C. Industry benchmarks and standards
- D. Return on IT security-related investments

Answer: D

Question #:119 - (Exam Topic 1)

Which of the following is the BEST key performance indicator (KPI) to measure the maturity of an organization's security incident handling process?

- A. The number of security incidents escalated to senior management
- B. The number of resolved security incidents
- C. The number of newly identified security incidents
- D. The number of recurring security incidents

Answer: B

Question #:120 - (Exam Topic 1)

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

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

Answer: B

Question #:121 - (Exam Topic 1)

A business unit is updating a risk register with assessment results for a key project. Which of the following is MOST important to capture in the register?

- A. The team that performed the risk assessment
- B. An assigned risk manager to provide oversight
- C. Action plans to address risk scenarios requiring treatment
- D. The methodology used to perform the risk assessment

Answer: B

Question #:122 - (Exam Topic 1)

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: A

Question #:123 - (Exam Topic 1)

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

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

Answer: B

Question #:124 - (Exam Topic 1)

Malware has recently affected an organization, The MOST effective way to resolve this situation and define a comprehensive risk treatment plan would be to perform:

- A. a gap analysis
- B. a root cause analysis.
- C. an impact assessment.
- D. a vulnerability assessment.

Answer: C

Question #:125 - (Exam Topic 1)

Which of the following will BEST quantify the risk associated with malicious users in an organization?

- A. Business impact analysis
- B. Risk analysis
- C. Threat risk assessment
- D. Vulnerability assessment

Answer: A

Question #:126 - (Exam Topic 1)

Which of the following is the BEST course of action to reduce risk impact?

A. Create an IT security policy.

- B. Implement corrective measures.
- C. Implement detective controls.
- D. Leverage existing technology

Answer: B

Question #:127 - (Exam Topic 1)

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

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

Answer: A

Question #:128 - (Exam Topic 1)

Which of the following is the MOST important outcome of reviewing the risk management process?

- A. Assuring the risk profile supports the IT objectives
- B. Improving the competencies of employees who performed the review
- C. Determining what changes should be nude to IS policies to reduce risk
- D. Determining that procedures used in risk assessment are appropriate

Answer: A

Question #:129 - (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

Question #:130 - (Exam Topic 1)

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

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

Answer: D

Question #:131 - (Exam Topic 1)

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

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

Answer: C

Question #:132 - (Exam Topic 1)

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

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

Answer: B

Question #:133 - (Exam Topic 1)

The PRIMARY objective of testing the effectiveness of a new control before implementation is to:

- A. ensure that risk is mitigated by the control.
- B. measure efficiency of the control process.
- C. confirm control alignment with business objectives.
- D. comply with the organization's policy.

Answer: C

Question #:134 - (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

Question #:135 - (Exam Topic 1)

The PRIMARY benefit of maintaining an up-to-date risk register is that it helps to:

- A. implement uniform controls for common risk scenarios.
- B. ensure business unit risk is uniformly distributed.
- C. build a risk profile for management review.
- D. quantify the organization's risk appetite.

Answer: C

Question #:136 - (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

Question #:137 - (Exam Topic 1)

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

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

Answer: C

Question #:138 - (Exam Topic 1)

A risk manager has determined there is excessive risk with a particular technology. Who is the BEST person to own the unmitigated risk of the technology?

- A. IT system owner
- B. Chief financial officer
- C. Chief risk officer
- D. Business process owner

Answer: D

Ouestion #:139 - (Exam Topic 1)

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

Question #:140 - (Exam Topic 1)

Which of the following is the BEST way to identify changes to the risk landscape?

- A. Internal audit reports
- B. Access reviews
- C. Threat modeling
- D. Root cause analysis

Answer: C

Question #:141 - (Exam Topic 1)

During an IT risk scenario review session, business executives question why they have been assigned ownership of IT-related risk scenarios. They feel IT risk is technical in nature and therefore should be owned by IT. Which of the following is the BEST way for the risk practitioner to address these concerns?

- A. Describe IT risk scenarios in terms of business risk.
- B. Recommend the formation of an executive risk council to oversee IT risk.
- C. Provide an estimate of IT system downtime if IT risk materializes.
- D. Educate business executives on IT risk concepts.

Answer: A

Question #:142 - (Exam Topic 1)

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

Question #:143 - (Exam Topic 1)

When updating the risk register after a risk assessment, which of the following is MOST important to include?

- A. Historical losses due to past risk events
- B. Cost to reduce the impact and likelihood
- C. Likelihood and impact of the risk scenario
- D. Actor and threat type of the risk scenario

Answer: C

Question #:144 - (Exam Topic 1)

A global organization is considering the acquisition of a competitor. Senior management has requested a review of the overall risk profile from the targeted organization. Which of the following components of this review would provide the MOST useful information?

- A. Risk appetite statement
- B. Enterprise risk management framework
- C. Risk management policies
- D. Risk register

Answer: D

Question #:145 - (Exam Topic 1)

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

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

Answer: B

Question #:146 - (Exam Topic 1)

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

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

Answer: B

Question #:147 - (Exam Topic 1)

Which of the following would be a risk practitioner'\$ 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

Question #:148 - (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 (KRls).

Answer: A

Question #:149 - (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

Question #:150 - (Exam Topic 1)

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

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

Answer: A

Question #:151 - (Exam Topic 1)

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

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

Answer: D

Question #:152 - (Exam Topic 1)

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

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

Answer: B

Question #:153 - (Exam Topic 1)

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

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

Answer: A

Question #:154 - (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

Question #:155 - (Exam Topic 1)

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

A. Customizing content for the audience

- B. Providing incentives to participants
- C. Mapping to a recognized standard
- D. Providing metrics for measurement

Answer: A

Ouestion #:156 - (Exam Topic 1)

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

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

Answer: D

Question #:157 - (Exam Topic 1)

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

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

Answer: D

Question #:158 - (Exam Topic 1)

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

- A. Maintain and review the classified data inventor.
- B. Implement mandatory encryption on data

- C. Conduct an awareness program for data owners and users.
- D. Define and implement a data classification policy

Answer: D

Question #:159 - (Exam Topic 1)

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

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

Answer: C

Question #:160 - (Exam Topic 1)

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

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

Answer: A

Question #:161 - (Exam Topic 1)

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

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

Answer: B

Question #:162 - (Exam Topic 1)

Which of the following would BEST help to ensure that suspicious network activity is identified?

- A. Analyzing intrusion detection system (IDS) logs
- B. Analyzing server logs
- C. Using a third-party monitoring provider
- D. Coordinating events with appropriate agencies

Answer: A

Question #:163 - (Exam Topic 1)

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

Question #:164 - (Exam Topic 1)

A risk practitioner is organizing a training session lo communicate risk assessment methodologies to ensure a consistent risk view within the organization Which of the following i< 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

Question #:165 - (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

Question #:166 - (Exam Topic 1)

The PRIMARY advantage of implementing an IT risk management framework is the:

- A. establishment of a reliable basis for risk-aware decision making.
- B. compliance with relevant legal and regulatory requirements.
- C. improvement of controls within the organization and minimized losses.
- D. alignment of business goals with IT objectives.

Answer: A

Question #:167 - (Exam Topic 1)

Which of the following attributes of a key risk indicator (KRI) is MOST important?

- A. Repeatable
- B. Automated
- C. Quantitative
- D. Qualitative

Answer: A

Question #:168 - (Exam Topic 1)

To implement the MOST effective monitoring of key risk indicators (KRIs), which of the following needs to be in place?

A. Threshold definition

- B. Escalation procedures
- C. Automated data feed
- D. Controls monitoring

Answer: A

Question #:169 - (Exam Topic 1)

A risk practitioner discovers several key documents detailing the design of a product currently in development have been posted on the Internet. What should be the risk practitioner's FIRST course of action?

- A. invoke the established incident response plan.
- B. Inform internal audit.
- C. Perform a root cause analysis
- D. Conduct an immediate risk assessment

Answer: A

Question #:170 - (Exam Topic 1)

Who is the MOST appropriate owner for newly identified IT risk?

- A. The manager responsible for IT operations that will support the risk mitigation efforts
- B. The individual with authority to commit organizational resources to mitigate the risk
- C. A project manager capable of prioritizing the risk remediation efforts
- D. The individual with the most IT risk-related subject matter knowledge

Answer: B

Question #:171 - (Exam Topic 1)

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

- A. Benchmark of industry standards
- B. Internal and external risk reports
- C. Recommendations from IT risk experts

D. Outcome of control self-assessments

Answer: B

Question #:172 - (Exam Topic 1)

When using a third party to perform penetration testing, which of the following is the MOST important control to minimize operational impact?

- A. Perform a background check on the vendor.
- B. Require the vendor to sign a nondisclosure agreement.
- C. Require the vendor to have liability insurance.
- D. Clearly define the project scope

Answer: D

Question #:173 - (Exam Topic 1)

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

Question #:174 - (Exam Topic 1)

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

Question #:175 - (Exam Topic 1)

Reviewing results from which of the following is the BEST way to identify information systems control deficiencies?

- A. Vulnerability and threat analysis
- B. Control remediation planning
- C. User acceptance testing (UAT)
- D. Control self-assessment (CSA)

Answer: D

Question #:176 - (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

Ouestion #:177 - (Exam Topic 1)

Risk mitigation procedures should include:

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

Answer: C

Question #:178 - (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

Question #:179 - (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

Question #:180 - (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

Question #:181 - (Exam Topic 1)

An organization has determined a risk scenario is outside the defined risk tolerance level. What should be the NEXT course of action?

A. Develop a compensating control.

- B. Allocate remediation resources.
- C. Perform a cost-benefit analysis.
- D. Identify risk responses

Answer: D

Question #:182 - (Exam Topic 1)

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

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

Answer: A

Question #:183 - (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

Question #:184 - (Exam Topic 1)

Which of the following roles would provide the MOST important input when identifying IT risk scenarios?

- A. Information security managers
- B. Internal auditors
- C. Business process owners

D. Operational risk managers

Answer: C

Question #:185 - (Exam Topic 1)

Which of the following provides the BEST evidence of the effectiveness of an organization's account provisioning process?

- A. User provisioning
- B. Role-based access controls
- C. Security log monitoring
- D. Entitlement reviews

Answer: B

Question #:186 - (Exam Topic 1)

IT risk assessments can BEST be used by management:

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

Answer: C

Question #:187 - (Exam Topic 1)

The MOST effective way to increase the likelihood that risk responses will be implemented is to:

- A. create an action plan
- B. assign ownership
- C. review progress reports
- D. perform regular audits.

Answer: B

Question #:188 - (Exam Topic 1)

In response to the threat of ransomware, an organization has implemented cybersecurity awareness activities. The risk practitioner's BEST recommendation to further reduce the impact of ransomware attacks would be to implement:

- A. two-factor authentication.
- B. continuous data backup controls.
- C. encryption for data at rest.
- D. encryption for data in motion.

Answer: B

Question #:189 - (Exam Topic 1)

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

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

Answer: B

Question #:190 - (Exam Topic 1)

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

Question #:191 - (Exam Topic 1)

Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?

- A. Ongoing availability of data
- B. Ability to aggregate data
- C. Ability to predict trends
- D. Availability of automated reporting systems

Answer: C

Question #:192 - (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

Question #:193 - (Exam Topic 1)

A risk practitioner has determined that a key control does not meet design expectations. Which of the following should be done NEXT?

- A. Document the finding in the risk register.
- B. Invoke the incident response plan.
- C. Re-evaluate key risk indicators.
- D. Modify the design of the control.

Answer: A

Question #:194 - (Exam Topic 1)

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

Question #:195 - (Exam Topic 1)

Which of the following would be- MOST helpful to understand the impact of a new technology system on an organization's current risk profile?

- A. Hire consultants specializing m the new technology.
- B. Review existing risk mitigation controls.
- C. Conduct a gap analysis.
- D. Perform a risk assessment.

Answer: D

Question #:196 - (Exam Topic 1)

Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery plan (DRP)?

- A. Number of users that participated in the DRP testing
- B. Number of issues identified during DRP testing
- C. Percentage of applications that met the RTO during DRP testing
- D. Percentage of issues resolved as a result of DRP testing

Answer: B

Question #:197 - (Exam Topic 1)

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

- A. Perform an m-depth code review with an expert
- B. Validate functionality by running in a test environment

- C. Implement a service level agreement.
- D. Utilize the change management process.

Answer: C

Question #:198 - (Exam Topic 1)

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: A

Question #:199 - (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

Question #:200 - (Exam Topic 1)

After a risk has been identified, who is in the BEST position to select the appropriate risk treatment option?

- A. The risk practitioner
- B. The business process owner
- C. The risk owner

D. The control owner

Answer: C

Question #:201 - (Exam Topic 1)

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

Question #:202 - (Exam Topic 1)

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

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

Answer: A

Ouestion #:203 - (Exam Topic 1)

Which of the following should be the PRIMARY consideration when assessing the automation of control monitoring?

- A. impact due to failure of control
- B. Frequency of failure of control
- C. Contingency plan for residual risk
- D. Cost-benefit analysis of automation

Answer: D

Question #:204 - (Exam Topic 1)

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

Question #:205 - (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

Ouestion #:206 - (Exam Topic 1)

Which of the following is the BEST way for a risk practitioner to help management prioritize risk response?

- A. Align business objectives to the risk profile.
- B. Assess risk against business objectives
- C. Implement an organization-specific risk taxonomy.
- D. Explain risk details to management.

Answer: B

Question #:207 - (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

Question #:208 - (Exam Topic 1)

An unauthorized individual has socially engineered entry into an organization's secured physical premises. Which of the following is the BEST way to prevent future occurrences?

- A. Employ security guards.
- B. Conduct security awareness training.
- C. Install security cameras.
- D. Require security access badges.

Answer: B

Topic 2, Pool B

Question #:1 - (Exam Topic 2)

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

Question #:2 - (Exam Topic 2)

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

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

Answer: D

Question #:3 - (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

Question #:4 - (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

Question #:5 - (Exam Topic 2)

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

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

Answer: D

Question #:6 - (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

Question #:7 - (Exam Topic 2)

A risk practitioner is reviewing a vendor contract and finds there is no clause to control privileged access to the organization's systems by vendor employees. Which of the following is the risk practitioner's BEST course

of action?

- A. Contact the control owner to determine if a gap in controls exists.
- B. Add this concern to the risk register and highlight it for management review.
- C. Report this concern to the contracts department for further action.
- D. Document this concern as a threat and conduct an impact analysis.

Answer: C

Question #:8 - (Exam Topic 2)

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: B

Question #:9 - (Exam Topic 2)

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

Question #:10 - (Exam Topic 2)

Which of the following is MOST important for a risk practitioner to verify when evaluating the effectiveness of an organization's existing controls?

A. Senior management has approved the control design.

- B. Inherent risk has been reduced from original levels.
- C. Residual risk remains within acceptable levels.
- D. Costs for control maintenance are reasonable.

Answer: C

Question #:11 - (Exam Topic 2)

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

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

Answer: C

Question #:12 - (Exam Topic 2)

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

Question #:13 - (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

Question #:14 - (Exam Topic 2)

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: C

Question #:15 - (Exam Topic 2)

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

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

Answer: A

Question #:16 - (Exam Topic 2)

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

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

Answer: B

Question #:17 - (Exam Topic 2)

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

Question #:18 - (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

Question #:19 - (Exam Topic 2)

An organization is planning to acquire a new financial system. Which of the following stakeholders would provide the MOST relevant information for analyzing the risk associated with the new IT solution?

- A. Project sponsor
- B. Process owner
- C. Risk manager
- D. Internal auditor

Answer: B

Question #:20 - (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

Question #:21 - (Exam Topic 2)

The PRIMARY objective for requiring an independent review of an organization's IT risk management process should be to:

- A. assess gaps in IT risk management operations and strategic focus.
- B. confirm that IT risk assessment results are expressed as business impact.
- C. verify implemented controls to reduce the likelihood of threat materialization.
- D. ensure IT risk management is focused on mitigating potential risk.

Answer: D

Question #:22 - (Exam Topic 2)

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: C

Question #:23 - (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

Question #:24 - (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: B

Question #:25 - (Exam Topic 2)

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: A

Question #:26 - (Exam Topic 2)

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

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

Answer: A

Question #:27 - (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

Question #:28 - (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

Question #:29 - (Exam Topic 2)

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

- A. identity 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

Question #:30 - (Exam Topic 2)

When reviewing a risk response strategy, senior management's PRIMARY focus should be placed on the:

- A. cost-benefit analysis.
- B. investment portfolio.
- C. key performance indicators (KPIs).
- D. alignment with risk appetite.

Answer: D

Question #:31 - (Exam Topic 2)

As part of an overall IT risk management plan, an IT risk register BEST helps management:

- A. align IT processes with business objectives.
- B. communicate the enterprise risk management policy.
- C. stay current with existing control status.
- D. understand the organizational risk profile.

Answer: D

Question #:32 - (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

Question #:33 - (Exam Topic 2)

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

- A. Relevant risk case studies
- B. Internal audit findings

- C. Risk assessment results
- D. Penetration testing results

Answer: C

Question #:34 - (Exam Topic 2)

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

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

Answer: C

Question #:35 - (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

Question #:36 - (Exam Topic 2)

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

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

Answer: D

Question #:37 - (Exam Topic 2)

Which of the following criteria is MOST important when developing a response to an attack that would compromise data?

- A. The recovery time objective (RTO)
- B. The likelihood of a recurring attack
- C. The organization's risk tolerance
- D. The business significance of the information

Answer: D

Question #:38 - (Exam Topic 2)

Controls should be defined during the design phase of system development because:

- A. it is more cost-effective to determine controls in the early design phase.
- B. structured analysis techniques exclude identification of controls.
- C. structured programming techniques require that controls be designed before coding begins.
- D. technical specifications are defined during this phase.

Answer: A

Question #:39 - (Exam Topic 2)

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: A

Question #:40 - (Exam Topic 2)

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

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

Answer: D

Question #:41 - (Exam Topic 2)

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

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

Answer: A

Question #:42 - (Exam Topic 2)

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

Question #:43 - (Exam Topic 2)

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

- A. Internal audit
- B. Control owner

- C. Senior management
- D. Risk manager

Answer: C

Question #:44 - (Exam Topic 2)

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

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

Answer: B

Question #:45 - (Exam Topic 2)

Whose risk tolerance matters MOST when making a risk decision?

- A. Customers who would be affected by a breach
- B. Auditors, regulators and standards organizations
- C. The business process owner of the exposed assets
- D. The information security manager

Answer: C

Question #:46 - (Exam Topic 2)

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

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

Answer: B

Question #:47 - (Exam Topic 2)

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

Question #:48 - (Exam Topic 2)

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

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

Answer: C

Question #:49 - (Exam Topic 2)

Who is responsible for IT security controls that are outsourced to an external service provider?

- A. Organization's information security manager
- B. Organization's risk function
- C. Service provider's IT management
- D. Service provider's information security manager

Answer: B

Question #:50 - (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

Question #:51 - (Exam Topic 2)

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

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

Answer: A

Question #:52 - (Exam Topic 2)

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

Question #:53 - (Exam Topic 2)

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

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

Answer: A

Question #:54 - (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

Question #:55 - (Exam Topic 2)

A risk assessment has identified increased losses associated with an IT risk scenario. It is MOST important for the risk practitioner to:

- A. update the risk rating.
- B. reevaluate inherent risk.
- C. develop new risk scenarios.
- D. implement additional controls.

Answer: D

Question #:56 - (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

Question #:57 - (Exam Topic 2)

The PRIMARY reason for periodic penetration testing of Internet-facing applications is to:

- A. ensure policy and regulatory compliance.
- B. assess the proliferation of new threats.
- C. verify Internet firewall control settings.
- D. identify vulnerabilities in the system.

Answer: C

Question #:58 - (Exam Topic 2)

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

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

Answer: A

Question #:59 - (Exam Topic 2)

The BEST way to test the operational effectiveness of a data backup procedure is to:

- A. conduct an audit of files stored offsite.
- B. interview employees to compare actual with expected procedures.
- C. inspect a selection of audit trails and backup logs.
- D. demonstrate a successful recovery from backup files.

Answer: D

Question #:60 - (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

Question #:61 - (Exam Topic 2)

The BEST criteria when selecting a risk response is the:

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

Answer: C

Question #:62 - (Exam Topic 2)

A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

- A. Regulatory requirements may differ in each country.
- B. Data sampling may be impacted by various industry restrictions.
- C. Business advertising will need to be tailored by country.
- D. The data analysis may be ineffective in achieving objectives.

Answer: A

Question #:63 - (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

Question #:64 - (Exam Topic 2)

After migrating a key financial system to a new provider, it was discovered that a developer could gain access to the production environment. Which of the following is the BEST way to mitigate the risk in this

situation?

- A. Escalate the issue to the service provider.
- B. Re-certify the application access controls.
- C. Remove the developer's access.
- D. Review the results of pre-migration testing.

Answer: B

Question #:65 - (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

Question #:66 - (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 nsk

Answer: A

Question #:67 - (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

Question #:68 - (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: B

Question #:69 - (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: D

Question #:70 - (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

Question #:71 - (Exam Topic 2)

A new regulator/ requirement imposes severe fines for data leakage involving customers' personally identifiable information (Pll). The risk practitioner has recommended avoiding the risk. Which of the following actions would BEST align with this recommendation?

- A. Reduce retention periods for Pll data.
- B. Move Pll to a highly-secured outsourced site.
- C. Modify business processes to stop collecting Pll.
- D. Implement strong encryption for Pll.

Answer: C

Question #:72 - (Exam Topic 2)

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

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

Answer: D

Question #:73 - (Exam Topic 2)

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

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

Answer: B

Question #:74 - (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: A

Question #:75 - (Exam Topic 2)

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

Question #:76 - (Exam Topic 2)

The design of procedures to prevent fraudulent transactions within an enterprise resource planning (ERP)

system should be based on:

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

Answer: D

Question #:77 - (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

Question #:78 - (Exam Topic 2)

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

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

Answer: D

Question #:79 - (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 low. medium and high.
- C. can be used m a cost-benefit analysts
- D. can be used to determine the indirect business impact.

Answer: C

Question #:80 - (Exam Topic 2)

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 (KRls)
- C. Changes to the team responsible for maintaining the register
- D. Completion of the latest internal audit

Answer: A

Question #:81 - (Exam Topic 2)

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: C

Question #:82 - (Exam Topic 2)

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

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

Answer: C

Question #:83 - (Exam Topic 2)

Which of the following should be the PRIMARY objective of a risk awareness training program?

- A. To enable risk-based decision making
- B. To promote awareness of the risk governance function
- C. To clarify fundamental risk management principles
- D. To ensure sufficient resources are available

Answer: A

Question #:84 - (Exam Topic 2)

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: C

Question #:85 - (Exam Topic 2)

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

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

Answer: B

Question #:86 - (Exam Topic 2)

The MOST essential content to include in an IT risk awareness program is how to:

- A. populate risk register entries and build a risk profile for management reporting.
- B. prioritize IT-related actions by considering risk appetite and risk tolerance.
- C. define the IT risk framework for the organization.
- D. comply with the organization's IT risk and information security policies.

Answer: D

Question #:87 - (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

Question #:88 - (Exam Topic 2)

An organization is preparing to transfer a large number of customer service representatives to the sales department. Of the following, who is responsible for mitigating the risk associated with residual system access?

- A. IT service desk manager
- B. Sales manager
- C. Customer service manager
- D. Access control manager

Answer: D

Question #:89 - (Exam Topic 2)

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

- A. A data extraction tool
- B. An access control list

- C. An intrusion detection system (IDS)
- D. An acceptable usage policy

Answer: C

Ouestion #:90 - (Exam Topic 2)

Which of the following is the MOST important responsibility of a risk owner?

- A. Testing control design
- B. Accepting residual risk
- C. Establishing business information criteria
- D. Establishing the risk register

Answer: B

Question #:91 - (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

Question #:92 - (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

Question #:93 - (Exam Topic 2)

Which of the following BEST reduces the probability of laptop theft?

- A. Cable lock
- B. Acceptable use policy
- C. Data encryption
- D. Asset tag with GPS

Answer: D

Question #:94 - (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

Question #:95 - (Exam Topic 2)

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

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

Answer: D

Question #:96 - (Exam Topic 2)

A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner's FIRST course of action?

- A. Update the KRI threshold.
- B. Recommend additional controls.
- C. Review incident handling procedures.
- D. Perform a root cause analysis.

Answer: D

Question #:97 - (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: D

Question #:98 - (Exam Topic 2)

Which of The following should be of GREATEST concern for an organization considering the adoption of a bring your own device (BYOD) initiative?

- A. Device corruption
- B. Data loss
- C. Malicious users
- D. User support

Answer: B

Question #:99 - (Exam Topic 2)

A risk owner should be the person accountable for:

- A. the risk management process
- B. managing controls.
- C. implementing actions.
- D. the business process.

Answer: D

Question #:100 - (Exam Topic 2)

What should a risk practitioner do FIRST when vulnerability assessment results identify a weakness in an application?

- A. Review regular control testing results.
- B. Recommend a penetration test.
- C. Assess the risk to determine mitigation needed.
- D. Analyze key performance indicators (KPIs).

Answer: C

Question #:101 - (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

Question #:102 - (Exam Topic 2)

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

- A. results of the review are accurately reported to management.
- B. identified findings are reviewed by the organization.

- C. results of the review are validated by internal audit.
- D. identified findings are approved by the vendor.

Answer: A

Question #:103 - (Exam Topic 2)

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

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

Answer: A

Question #:104 - (Exam Topic 2)

An organization has completed a project to implement encryption on all databases that host customer data. Which of the following elements of the risk register should be updated the reflect this change?

- A. Risk likelihood
- B. Inherent risk
- C. Risk appetite
- D. Risk tolerance

Answer: B

Ouestion #:105 - (Exam Topic 2)

An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?

- A. Number of customer records held
- B. Number of databases that host customer data
- C. Number of encrypted customer databases
- D. Number of staff members having access to customer data

Answer: B

Question #:106 - (Exam Topic 2)

A risk practitioner recently discovered that sensitive data from the production environment is required for testing purposes in non-production environments. Which of the following i the BEST recommendation to address this situation?

- A. Enable data encryption in the test environment
- B. Implement equivalent security in the test environment.
- C. Prevent the use of production data for test purposes
- D. Mask data before being transferred to the test environment.

Answer: B

Question #:107 - (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

Question #:108 - (Exam Topic 2)

Which of the following can be used to assign a monetary value to risk?

- A. Annual loss expectancy (ALE)
- B. Business impact analysis
- C. Cost-benefit analysis
- D. Inherent vulnerabilities

Answer: A

Question #:109 - (Exam Topic 2)

Who is accountable for risk treatment?

- A. Enterprise risk management team
- B. Risk mitigation manager
- C. Business process owner
- D. Risk owner

Answer: C

Question #:110 - (Exam Topic 2)

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

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

Answer: B

Question #:111 - (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

Question #:112 - (Exam Topic 2)

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

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

Answer: A

Question #:113 - (Exam Topic 2)

The effectiveness of a control has decreased. What is the MOST likely effect on the associated risk?

- A. The risk impact changes.
- B. The risk classification changes.
- C. The inherent risk changes.
- D. The residual risk changes.

Answer: D

Question #:114 - (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: B

Question #:115 - (Exam Topic 2)

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

Question #:116 - (Exam Topic 2)

A monthly payment report is generated from the enterprise resource planning (ERP) software to validate data against the old and new payroll systems. What is the BEST way to mitigate the risk associated with data integrity loss in the new payroll system after data migration?

- A. Compare new system reports with functional requirements.
- B. Compare encrypted data with checksums.
- C. Compare results of user acceptance testing (UAT) with the testing criteria.
- D. Compare processing output from both systems using the previous month's data.

Answer: D

Question #:117 - (Exam Topic 2)

An organization has granted a vendor access to its data in order to analyze customer behavior. Which of the following would be the MOST effective control to mitigate the risk of customer data leakage?

- A. Enforce criminal background checks.
- B. Mask customer data fields.
- C. Require vendor to sign a confidentiality agreement.
- D. Restrict access to customer data on a "need to know" basis.

Answer: B

Question #:118 - (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

Question #:119 - (Exam Topic 2)

Mapping open risk issues to an enterprise risk heat map BEST facilitates:

- A. risk response.
- B. control monitoring.
- C. risk identification.
- D. risk ownership.

Answer: D

Question #:120 - (Exam Topic 2)

The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

- A. availability of fault tolerant software.
- B. strategic plan for business growth.
- C. vulnerability scan results of critical systems.
- D. redundancy of technical infrastructure.

Answer: D

Question #:121 - (Exam Topic 2)

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

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

- A. Project Charlie
- B. Project Bravo

- C. Project Alpha
- D. Project Delta

Answer: A

Question #:122 - (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

Question #:123 - (Exam Topic 2)

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

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

Answer: D

Question #:124 - (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

Question #:125 - (Exam Topic 2)

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

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

Answer: D

Question #:126 - (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

Ouestion #:127 - (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: D

Question #:128 - (Exam Topic 2)

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

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

Answer: B

Question #:129 - (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

Ouestion #:130 - (Exam Topic 2)

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

Objectives are confirmed with the business owner.

Control owners approve control changes.

End-user acceptance testing has been conducted.

Performance information in the log is encrypted.

D

Question #:131 - (Exam Topic 2)

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

A. Identify systems that are vulnerable to being exploited by the attack.

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

Answer: A

Question #:132 - (Exam Topic 2)

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

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

Answer: D

Question #:133 - (Exam Topic 2)

Which of the following should management consider when selecting a risk mitigation option?

- A. Maturity of the enterprise architecture
- B. Cost of control implementation
- C. Reliability of key performance indicators (KPIs)
- D. Reliability of key risk indicators (KPIs)

Answer: B

Question #:134 - (Exam Topic 2)

The MOST important reason to aggregate results from multiple risk assessments on interdependent information systems is to:

- A. establish overall impact to the organization
- B. efficiently manage the scope of the assignment
- C. identify critical information systems

D. facilitate communication to senior management

Answer: A

Question #:135 - (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

Question #:136 - (Exam Topic 2)

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: D

Question #:137 - (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

Question #:138 - (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

Question #:139 - (Exam Topic 2)

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

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

Answer: D

Question #:140 - (Exam Topic 2)

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

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

Answer: D

Question #:141 - (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: A

Question #:142 - (Exam Topic 2)

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

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

Answer: A

Question #:143 - (Exam Topic 2)

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: C

Question #:144 - (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

Question #:145 - (Exam Topic 2)

Which of the following is MOST effective in continuous risk management process improvement?

- A. Periodic assessments
- B. Change management
- C. Awareness training
- D. Policy updates

Answer: C

Question #:146 - (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: D

Question #:147 - (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

Question #:148 - (Exam Topic 2)

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

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

Answer: B

Question #:149 - (Exam Topic 2)

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

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

Answer: C

Question #:150 - (Exam Topic 2)

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

Question #:151 - (Exam Topic 2)

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

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

Answer: A

Question #:152 - (Exam Topic 2)

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

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

Answer: A

Question #:153 - (Exam Topic 2)

The MAIN goal of the risk analysis process is to determine the:

- A. potential severity of impact
- B. frequency and magnitude of loss
- C. control deficiencies
- D. threats and vulnerabilities

Answer: B

Question #:154 - (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

Question #:155 - (Exam Topic 2)

Accountability for a particular risk is BEST represented in a:

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

Answer: D

Question #:156 - (Exam Topic 2)

Which of the following BEST measures the impact of business interruptions caused by an IT service outage?

- A. Sustained financial loss
- B. Cost of remediation efforts
- C. Duration of service outage
- D. Average time to recovery

Answer: D

Question #:157 - (Exam Topic 2)

The PRIMARY purpose of vulnerability assessments is to:

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

Answer: D

Question #:158 - (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

Question #:159 - (Exam Topic 2)

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

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

Answer: A

Question #:160 - (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

Question #:161 - (Exam Topic 2)

Which of the following is the PRIMARY reason for monitoring activities performed in a production database environment?

A. Ensuring that database changes are correctly applied

- B. Enforcing that changes are authorized
- C. Deterring illicit actions of database administrators
- D. Preventing system developers from accessing production data

Answer: C

Question #:162 - (Exam Topic 2)

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 (KRls) 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

Question #:163 - (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: D

Ouestion #:164 - (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

Question #:165 - (Exam Topic 2)

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

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

Answer: B

Question #:166 - (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

Ouestion #:167 - (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

Question #:168 - (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: A

Question #:169 - (Exam Topic 2)

Which of the following BEST indicates effective information security incident management?

- A. Monthly trend of information security-related incidents
- B. Average time to identify critical information security incidents
- C. Frequency of information security incident response plan testing
- D. Percentage of high risk security incidents

Answer: C

Question #:170 - (Exam Topic 2)

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

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

Answer: A

Question #:171 - (Exam Topic 2)

Which of the following should be considered when selecting a risk response?

- A. Risk scenarios analysis
- B. Risk response costs
- C. Risk factor awareness
- D. Risk factor identification

Answer: B

Question #:172 - (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

Question #:173 - (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: C

Question #:174 - (Exam Topic 2)

Which of the following is performed after a risk assessment is completed?

- A. Defining risk taxonomy
- B. Identifying vulnerabilities

- C. Conducting an impact analysis
- D. Defining risk response options

Answer: C

Question #:175 - (Exam Topic 2)

Which of the following is MOST important to sustainable development of secure IT services?

- A. Security training for systems development staff
- B. \Well-documented business cases
- C. Security architecture principles
- D. Secure coding practices

Answer: C

Question #:176 - (Exam Topic 2)

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

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

Answer: A

Question #:177 - (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

Question #:178 - (Exam Topic 2)

Within the three lines of defense model, the accountability for the system of internal control resides with:

- A. the chief information officer (CIO).
- B. the board of directors
- C. enterprise risk management
- D. the risk practitioner

Answer: B

Question #:179 - (Exam Topic 2)

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

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

Answer: D

Question #:180 - (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

Question #:181 - (Exam Topic 2)

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

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

Answer: A

Question #:182 - (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

Question #:183 - (Exam Topic 2)

An IT organization is replacing the customer relationship management (CRM) system. Who should own the risk associated with customer data leakage caused by insufficient IT security controls for the new system?

- A. Chief information security officer
- B. Business process owner
- C. Chief risk officer
- D. IT controls manager

Answer: B

Question #:184 - (Exam Topic 2)

Which of the following should be the MAIN consideration when validating an organization's risk appetite?

A. Comparison against regulations

- B. Maturity of the risk culture
- C. Capacity to withstand loss
- D. Cost of risk mitigation options

Answer: B

Question #:185 - (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

Question #:186 - (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: C

Question #:187 - (Exam Topic 2)

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

Question #:188 - (Exam Topic 2)

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: B

Question #:189 - (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: B

Question #:190 - (Exam Topic 2)

Which of the following is the BEST indicator of the effectiveness of a control action plan's implementation?

- A. Increased number of controls
- B. Reduced risk level
- C. Increased risk appetite
- D. Stakeholder commitment

Answer: B

Question #:191 - (Exam Topic 2)

Which of the following BEST enables the risk profile to serve as an effective resource to support business objectives?

- A. Engaging external risk professionals to periodically review the risk
- B. Prioritizing global standards over local requirements in the risk profile
- C. Updating the risk profile with risk assessment results
- D. Assigning quantitative values to qualitative metrics in the risk register

Answer: A

Question #:192 - (Exam Topic 2)

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

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

Answer: D

Question #:193 - (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

Question #:194 - (Exam Topic 2)

An organization uses a vendor to destroy hard drives. Which of the following would BEST reduce the risk of data leakage?

- A. Require the vendor to degauss the hard drives
- B. Implement an encryption policy for the hard drives.
- C. Require confirmation of destruction from the IT manager.
- D. Use an accredited vendor to dispose of the hard drives.

Answer: A

Question #:195 - (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: B

Question #:196 - (Exam Topic 2)

An organization's risk practitioner learns a new third-party system on the corporate network has introduced vulnerabilities that could compromise corporate IT systems. What should the risk practitioner do

FIRST?

- A. Confirm the vulnerabilities with the third party
- B. Identify procedures to mitigate the vulnerabilities.
- C. Notify information security management.
- D. Request IT to remove the system from the network.

Answer: B

Question #:197 - (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

Question #:198 - (Exam Topic 2)

During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?

- A. Implement compensating controls to reduce residual risk
- B. Escalate the issue to senior management
- C. Discuss risk mitigation options with the risk owner.
- D. Certify the control after documenting the concern.

Answer: A

Question #:199 - (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

Question #:200 - (Exam Topic 2)

What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium C	C Low C	C, Low
Tango Cy.	Medium Cy.	Cy. Low Cy.	Medium
Uniform	High O	High O	High O
Victor %	High	Medium	Medium

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

Answer: A

Question #:201 - (Exam Topic 2)

Which of the following provides the MOST important information to facilitate a risk response decision?

- A. Audit findings
- B. Risk appetite
- C. Key risk indicators
- D. Industry best practices

Answer: B

Question #:202 - (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

Question #:203 - (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

Question #:204 - (Exam Topic 2)

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

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

Answer: C

Question #:205 - (Exam Topic 2)

Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is aligned to business requirements?

- A. Total cost to support the policy
- B. Number of exceptions to the policy
- C. Total cost of policy breaches
- D. Number of inquiries regarding the policy

Answer: C

Question #:206 - (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

Question #:207 - (Exam Topic 2)

An organization has opened a subsidiary in a foreign country. Which of the following would be the BEST way to measure the effectiveness of the subsidiary's IT systems controls?

- A. Implement IT systems in alignment with business objectives.
- B. Review metrics and key performance indicators (KPIs).
- C. Review design documentation of IT systems.
- D. Evaluate compliance with legal and regulatory requirements.

Answer: D

Question #:208 - (Exam Topic 2)

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

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

Answer: B

Question #:209 - (Exam Topic 2)

The BEST key performance indicator (KPI) for monitoring adherence to an organization's user accounts provisioning practices is the percentage of:

A. accounts without documented approval

- B. user accounts with default passwords
- C. active accounts belonging to former personnel
- D. accounts with dormant activity.

Answer: A

Question #:210 - (Exam Topic 2)

The PRIMARY benefit of conducting continuous monitoring of access controls is the ability to identify:

- A. inconsistencies between security policies and procedures
- B. possible noncompliant activities that lead to data disclosure
- C. leading or lagging key risk indicators (KRIs)
- D. unknown threats to undermine existing access controls

Answer: B

Question #:211 - (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

Question #:212 - (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

Question #:213 - (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

Question #:214 - (Exam Topic 2)

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: A

Question #:215 - (Exam Topic 2)

Which of the following provides the MOST important information to facilitate a risk response decision?

- A. Audit findings
- B. Risk appetite
- C. Key risk indicators
- D. Industry best practices

Answer: B

Question #:216 - (Exam Topic 2)

A risk owner has identified a risk with high impact and very low likelihood. The potential loss is covered by insurance. Which of the following should the risk practitioner do NEXT?

- A. Recommend avoiding the risk.
- B. Validate the risk response with internal audit.
- C. Update the risk register.
- D. Evaluate outsourcing the process.

Answer: B

Question #:217 - (Exam Topic 2)

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

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

Answer: B

Question #:218 - (Exam Topic 2)

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

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

Answer: C

Question #:219 - (Exam Topic 2)

Which of the following is a crucial component of a key risk indicator (KRI) to ensure appropriate action is taken to mitigate risk?

- A. Management intervention
- B. Risk appetite
- C. Board commentary
- D. Escalation triggers

Answer: D

Question #:220 - (Exam Topic 2)

To help identify high-risk situations, an organization should:

- A. continuously monitor the environment
- B. develop key performance indicators (KPIs).
- C. maintain a risk matrix.
- D. maintain a risk register.

Answer: A

Question #:221 - (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: A

Question #:222 - (Exam Topic 2)

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

- A. rolled back changes below management's thresholds.
- B. change-related exceptions per month.

- C. the average implementation time for changes.
- D. number of user stories approved for implementation.

Answer: B

Question #:223 - (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

Question #:224 - (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

Question #:225 - (Exam Topic 2)

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

- A. Cost-benefit analysis of running the current business
- B. Cost of regulatory compliance
- C. Projected impact of current business on future business

D. Expected costs for recovering the business

Answer: C

Question #:226 - (Exam Topic 2)

Which of the following should a risk practitioner do FIRST when an organization decides to use a cloud service?

- A. Review the vendor selection process and vetting criteria.
- B. Assess whether use of service falls within risk tolerance thresholds.
- C. Establish service level agreements (SLAs) with the vendor.
- D. Check the contract for appropriate security risk and control provisions.

Answer: D

Question #:227 - (Exam Topic 2)

Which of The following is the MOST relevant information to include in a risk management strategy?

- A. Quantified risk triggers
- B. Cost of controls
- C. Regulatory requirements
- D. Organizational goals

Answer: D

Question #:228 - (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

Question #:229 - (Exam Topic 2)

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

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

Answer: C

Question #:230 - (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

Question #:231 - (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 (KPls)
- B. Key risk indicators (KRIs)
- C. Centralized risk register
- D. Risk heat map

Answer: D

Question #:232 - (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

Question #:233 - (Exam Topic 2)

An organization's risk tolerance should be defined and approved by which of the following?

- A. The chief risk officer (CRO)
- B. The board of directors
- C. The chief executive officer (CEO)
- D. The chief information officer (CIO)

Answer: B

Question #:234 - (Exam Topic 2)

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

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

Answer: B

Question #:235 - (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

Question #:236 - (Exam Topic 2)

Which of the following risk scenarios would be the GREATEST concern as a result of a single sign-on implementation?

- A. User access may be restricted by additional security.
- B. Unauthorized access may be gained to multiple systems.
- C. Security administration may become more complex.
- D. User privilege changes may not be recorded.

Answer: B

Question #:237 - (Exam Topic 2)

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

- A. The scenarios are based on industry best practice.
- B. The scenarios focus on current vulnerabilities.
- C. The scenarios are relevant to the organization.
- D. The scenarios include technical consequences.

Answer: C

Question #:238 - (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

Question #:239 - (Exam Topic 2)

In an organization where each division manages risk independently, which of the following would BEST enable management of risk at the enterprise level?

- A. A standardized risk taxonomy
- B. A list of control deficiencies
- C. An enterprise risk ownership policy
- D. An updated risk tolerance metric

Answer: A

Question #:240 - (Exam Topic 2)

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

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

Answer: A

Question #:241 - (Exam Topic 2)

An organization plans to migrate sensitive information to a public cloud infrastructure. Which of the following is the GREATEST security risk in this scenario?

- A. Data may be commingled with other tenants' data.
- B. System downtime does not meet the organization's thresholds.
- C. The infrastructure will be managed by the public cloud administrator.
- D. The cloud provider is not independently certified.

Answer: A

Question #:242 - (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

Question #:243 - (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

Question #:244 - (Exam Topic 2)

Which of the following would provide the MOST comprehensive information for updating an organization's risk register?

- A. Results of the latest risk assessment
- B. Results of a risk forecasting analysis
- C. A review of compliance regulations
- D. Findings of the most recent audit

Answer: A

Question #:245 - (Exam Topic 2)

Which of the following is MOST influential when management makes risk response decisions?

- A. Risk appetite
- B. Audit risk
- C. Residual risk
- D. Detection risk

Answer: C

Question #:246 - (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

Question #:247 - (Exam Topic 2)

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: D

Question #:248 - (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

Question #:249 - (Exam Topic 2)

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

Question #:250 - (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

Question #:251 - (Exam Topic 2)

Prior to selecting key performance indicators (KPIs), itis 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

Question #:252 - (Exam Topic 2)

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

Question #:253 - (Exam Topic 2)

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

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

Answer: D

Question #:254 - (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

Question #:255 - (Exam Topic 2)

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

Question #:256 - (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

Question #:257 - (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

Question #:258 - (Exam Topic 2)

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

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

Answer: A

Question #:259 - (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

Question #:260 - (Exam Topic 2)

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 anal/sis 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: A

Question #:261 - (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

Question #:262 - (Exam Topic 2)

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

Vulnerability analysis

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

Answer: C

Question #:263 - (Exam Topic 2)

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

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

Answer: C

Question #:264 - (Exam Topic 2)

The PRIMARY purpose of a maturity model is to compare the:

- A. current state of key processes to their desired state.
- B. actual KPIs with target KPIs.
- C. organization to industry best practices.
- D. organization to peers.

Answer: A

Question #:265 - (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

Question #:266 - (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

Question #:267 - (Exam Topic 2)

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

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

Answer: B

Question #:268 - (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: A

Question #:269 - (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

Question #:270 - (Exam Topic 2)

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: D

Question #:271 - (Exam Topic 2)

The PRIMARY benefit associated with key risk indicators (KRls) 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

Question #:272 - (Exam Topic 2)

Which of the following BEST promotes commitment to controls?

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

Answer: A

Question #:273 - (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: B

Question #:274 - (Exam Topic 2)

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

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

Answer: A

Question #:275 - (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

Question #:276 - (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 whistlebtower reports of noncompliance.
- D. Monitor user software download activity.

Answer: B

Question #:277 - (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

Question #:278 - (Exam Topic 2)

Which of the following should be initiated when a high number of noncompliant conditions are observed during review of a control procedure?

- A. Disciplinary action
- B. A control self-assessment
- C. A review of the awareness program
- D. Root cause analysis

Answer: D

Question #:279 - (Exam Topic 2)

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

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

Answer: C

Question #:280 - (Exam Topic 2)

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

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

Answer: D

Question #:281 - (Exam Topic 2)

The MAIN reason for creating and maintaining a risk register is to:

A. assess effectiveness of different projects.

- B. define the risk assessment methodology.
- C. ensure assets have low residual risk.
- D. account for identified key risk factors.

Answer: D

Question #:282 - (Exam Topic 2)

When prioritizing risk response, management should FIRST:

- A. evaluate the organization s ability and expertise to implement the solution.
- B. evaluate the risk response of similar organizations.
- C. address high risk factors that have efficient and effective solutions.
- D. determine which risk factors have high remediation costs

Answer: C

Question #:283 - (Exam Topic 2)

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

Question #:284 - (Exam Topic 2)

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: D

Question #:285 - (Exam Topic 2)

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

Question #:286 - (Exam Topic 2)

Which of the following is the BEST measure of the effectiveness of an employee deprovisioning process?

- A. Number of days taken to remove access after staff separation dates
- B. Number of days taken for IT to remove access after receipt of HR instructions
- C. Number of termination requests processed per reporting period
- D. Number of days taken for HR to provide instructions to IT after staff separation dates

Answer: A

Question #:287 - (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

Question #:288 - (Exam Topic 2)

An organization has engaged a third party to provide an Internet gateway encryption service that protects sensitive data uploaded to a cloud service. This is an example of risk:

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

Answer: A

Question #:289 - (Exam Topic 2)

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: D

Question #:290 - (Exam Topic 2)

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

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

Answer: B

Question #:291 - (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

Question #:292 - (Exam Topic 2)

Which of the following is MOST important when defining controls?

- A. Identifying monitoring mechanisms
- B. Including them in the risk register
- C. Aligning them with business objectives
- D. Prototyping compensating controls

Answer: C

Question #:293 - (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

Question #:294 - (Exam Topic 2)

A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (Pll). 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

Question #:295 - (Exam Topic 2)

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: B

Question #:296 - (Exam Topic 2)

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

Question #:297 - (Exam Topic 2)

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

Question #:298 - (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

Question #:299 - (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

Question #:300 - (Exam Topic 2)

Which of The following will BEST communicate the importance of risk mitigation initiatives to senior management?

- A. Business case
- B. Balanced scorecard
- C. Industry standards
- D. Heat map

Answer: A

Question #:301 - (Exam Topic 2)

Prudent business practice requires that risk appetite not exceed:

- A. inherent risk.
- B. risk tolerance.
- C. risk capacity.
- D. residual risk.

Answer: C

Question #:302 - (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

Question #:303 - (Exam Topic 2)

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: D

Question #:304 - (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: A

Question #:305 - (Exam Topic 2)

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

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

Answer: C

Question #:306 - (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

Question #:307 - (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

Question #:308 - (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

Question #:309 - (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

Question #:310 - (Exam Topic 2)

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

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

Answer: C

Question #:311 - (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

Question #:312 - (Exam Topic 2)

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

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

Answer: B

Ouestion #:313 - (Exam Topic 2)

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

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

Answer: B

Question #:314 - (Exam Topic 2)

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

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

Answer: B

Question #:315 - (Exam Topic 2)

Which of the following controls would BEST reduce the likelihood of a successful network attack through social engineering?

- A. Automated controls
- B. Security awareness training
- C. Multifactor authentication
- D. Employee sanctions

Answer: B

Question #:316 - (Exam Topic 2)

Which of the following is the MOST important information to be communicated during security awareness training?

- A. Management's expectations
- B. Corporate risk profile
- C. Recent security incidents
- D. The current risk management capability

Answer: A

Question #:317 - (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

Question #:318 - (Exam Topic 2)

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: A

Question #:319 - (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

Question #:320 - (Exam Topic 2)

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

- A. Risk magnitude
- B. Incident probability

- C. Risk appetite
- D. Cost-benefit analysis

Answer: B

Question #:321 - (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

Question #:322 - (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: D

Question #:323 - (Exam Topic 2)

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

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

Answer: C

Question #:324 - (Exam Topic 2)

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

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

Answer: A

Question #:325 - (Exam Topic 2)

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

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

Answer: D

Question #:326 - (Exam Topic 2)

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

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

Answer: A

Question #:327 - (Exam Topic 2)

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

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

Answer: A

Question #:328 - (Exam Topic 2)

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

Question #:329 - (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

Question #:330 - (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

Question #:331 - (Exam Topic 2)

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

Question #:332 - (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 10 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

Question #:333 - (Exam Topic 2)

A risk practitioner has learned that an effort to implement a risk mitigation action plan has stalled due to lack of funding. The risk practitioner should report that the associated risk has been:

- A. mitigated
- B. accepted

- C. avoided
- D. deferred

Answer: B

Question #:334 - (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

Question #:335 - (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

Question #:336 - (Exam Topic 2)

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

Question #:337 - (Exam Topic 2)

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

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

Answer: B

Question #:338 - (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

Question #:339 - (Exam Topic 2)

An organization has outsourced a critical process involving highly regulated data to a third party with servers located in a foreign country. Who is accountable for the confidentiality of this data?

- A. Third-party data custodian
- B. Data custodian
- C. Regional office executive
- D. Data owner

Answer: D

Question #:340 - (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

Question #:341 - (Exam Topic 2)

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

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

Answer: B

Question #:342 - (Exam Topic 2)

Which of the following is the MOST effective way to mitigate identified risk scenarios?

- A. Assign ownership of the risk response plan
- B. Provide awareness in early detection of risk.
- C. Perform periodic audits on identified risk.
- D. areas Document the risk tolerance of the organization.

Answer: A

Question #:343 - (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

Question #:344 - (Exam Topic 2)

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: A

Question #:345 - (Exam Topic 2)

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

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

Answer: D

Question #:346 - (Exam Topic 2)

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

A. Develop a business impact analysis (6IA).

- B. Define recovery time objectives (RTO).
- C. Analyze capability maturity model gaps.
- D. Simulate a disaster recovery.

Answer: D

Question #:347 - (Exam Topic 2)

Which of the following should be a risk practitioner's NEXT action after identifying a high probability of data loss in a system?

- A. Enhance the security awareness program.
- B. Increase the frequency of incident reporting.
- C. Purchase cyber insurance from a third party.
- D. Conduct a control assessment.

Answer: D

Question #:348 - (Exam Topic 2)

Which of the following is the BEST way for a risk practitioner to verify that management has addressed control issues identified during a previous external audit?

- A. Interview control owners.
- B. Observe the control enhancements in operation.
- C. Inspect external audit documentation.
- D. Review management's detailed action plans.

Answer: B

Ouestion #:349 - (Exam Topic 2)

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

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

Answer: C

Question #:350 - (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

Question #:351 - (Exam Topic 2)

An organization has decided to outsource a web application, and customer data will be stored in the vendor's public cloud. To protect customer data, it is MOST important to ensure which of the following?

- A. The organization's incident response procedures have been updated.
- B. The vendor stores the data in the same jurisdiction.
- C. Administrative access is only held by the vendor.
- D. The vendor's responsibilities are defined in the contract.

Answer: D

Question #:352 - (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

Question #:353 - (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

Question #:354 - (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

Question #:355 - (Exam Topic 2)

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

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

Answer: C

Question #:356 - (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

Question #:357 - (Exam Topic 2)

A risk practitioner has been notified that an employee sent an email in error containing customers' personally identifiable information (Pll). 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

Question #:358 - (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

Question #:359 - (Exam Topic 2)

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: B

Question #:360 - (Exam Topic 2)

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

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

Answer: A

Question #:361 - (Exam Topic 2)

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

Question #:362 - (Exam Topic 2)

Quantifying the value of a single asset helps the organization to understand the:

- A. overall effectiveness of risk management
- B. consequences of risk materializing
- C. necessity of developing a risk strategy,
- D. organization s risk threshold.

Answer: B

Question #:363 - (Exam Topic 2)

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

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

Answer: B

Question #:364 - (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

Question #:365 - (Exam Topic 2)

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

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

Answer: C

Question #:366 - (Exam Topic 2)

A key risk indicator (KRI) indicates a reduction in the percentage of appropriately patched servers. Which of the following is the risk practitioner's BEST course of action?

- A. Determine changes in the risk level.
- B. Outsource the vulnerability management process.
- C. Review the patch management process.
- D. Add agenda item to the next risk committee meeting.

Answer: C

Question #:367 - (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

Question #:368 - (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: C

Question #:369 - (Exam Topic 2)

Which of the following is the BEST way to promote adherence to the risk tolerance level set by management?

- A. Defining expectations in the enterprise risk policy
- B. Increasing organizational resources to mitigate risks
- C. Communicating external audit results

D. Avoiding risks that could materialize into substantial losses

Answer: A

Question #:370 - (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 (B1A)
- C. Control catalog
- D. Risk register

Answer: D

Question #:371 - (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

Question #:372 - (Exam Topic 2)

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

- A. Independent audit report
- B. Control self-assessment
- C. Key performance indicators (KPIs)
- D. Service level agreements (SLAs)

Answer: A

Question #:373 - (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

Question #:374 - (Exam Topic 2)

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

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

Answer: B

Question #:375 - (Exam Topic 2)

Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?

- A. Piloting courses with focus groups
- B. Using reputable third-party training programs
- C. Reviewing content with senior management
- D. Creating modules for targeted audiences

Answer: D

Question #:376 - (Exam Topic 2)

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

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

Answer: C

Question #:377 - (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

Ouestion #:378 - (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

Question #:379 - (Exam Topic 2)

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

Question #:380 - (Exam Topic 2)

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

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

Answer: B

Question #:381 - (Exam Topic 2)

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

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

Answer: A

Question #:382 - (Exam Topic 2)

During the initial risk identification process for a business application, it is MOST important to include which of the following stakeholders?

- A. Business process owners
- B. Business process consumers
- C. Application architecture team
- D. Internal audit

Answer: A

Question #:383 - (Exam Topic 2)

Which of the following is the GREATEST concern when an organization uses a managed security service provider as a firewall administrator?

- A. Exposure of log data
- B. Lack of governance
- C. Increased number of firewall rules
- D. Lack of agreed-upon standards

Answer: B

Question #:384 - (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: C

Question #:385 - (Exam Topic 2)

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

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

Answer: C

Question #:386 - (Exam Topic 2)

An IT license audit has revealed that there are several unlicensed copies of co be 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

Question #:387 - (Exam Topic 2)

Which of the following observations would be GREATEST concern to a risk practitioner reviewing the implementation status of management action plans?

- A. Management has not determined a final implementation date.
- B. Management has not completed an early mitigation milestone.
- C. Management has not secured resources for mitigation activities.
- D. Management has not begun the implementation.

Answer: C

Question #:388 - (Exam Topic 2)

A risk practitioner has just learned about new done 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

Question #:389 - (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

Question #:390 - (Exam Topic 2)

Which of the following is the MOST important enabler of effective risk management?

- A. User awareness of policies and procedures
- B. Implementation of proper controls
- C. Senior management support
- D. Continuous monitoring of threats and vulnerabilities

Answer: C

Question #:391 - (Exam Topic 2)

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

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

Answer: D

Question #:392 - (Exam Topic 2)

Which of the following is an IT business owner's BEST course of action following an unexpected increase in emergency changes?

- A. Evaluating the impact to control objectives
- B. Conducting a root cause analysis
- C. Validating the adequacy of current processes
- D. Reconfiguring the IT infrastructure

Answer: B

Question #:393 - (Exam Topic 2)

Due to a change in business processes, an identified risk scenario no longer requires mitigation. Which of the following is the MOST important reason the risk should remain in the risk register?

- A. To support regulatory requirements
- B. To prevent the risk scenario in the current environment
- C. To monitor for potential changes to the risk scenario
- D. To track historical risk assessment results

Answer: D

Question #:394 - (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

Question #:395 - (Exam Topic 2)

Which of the following is the FIRST step in risk assessment?

- A. Review risk governance
- B. Asset identification
- C. Identify risk factors
- D. Inherent risk identification

Answer: B

Question #:396 - (Exam Topic 2)

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

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

Answer: A

Question #:397 - (Exam Topic 2)

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

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

Answer: C

Question #:398 - (Exam Topic 2)

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

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

Answer: A

Question #:399 - (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

Question #:400 - (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

Question #:401 - (Exam Topic 2)

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

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

Answer: B

Question #:402 - (Exam Topic 2)

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

- A. To update risk ownership
- B. To review the risk acceptance with new stakeholders
- C. To ensure risk levels have not changed

D. To ensure controls are still operating effectively

Answer: C

Question #:403 - (Exam Topic 2)

Which of the following would be MOST useful to senior management when determining an appropriate risk response?

- A. A comparison of current risk levels with established tolerance
- B. A comparison of cost variance with defined response strategies
- C. A comparison of current risk levels with estimated inherent risk levels
- D. A comparison of accepted risk scenarios associated with regulatory compliance

Answer: A

Question #:404 - (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: A

Question #:405 - (Exam Topic 2)

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

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

Answer: C

Question #:406 - (Exam Topic 2)

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

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

Answer: C

Question #:407 - (Exam Topic 2)

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

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

Answer: A

Question #:408 - (Exam Topic 2)

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

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

Answer: D

Question #:409 - (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

Question #:410 - (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

Question #:411 - (Exam Topic 2)

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

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

Answer: B

Question #:412 - (Exam Topic 2)

When testing the security of an IT system, il 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

Question #:413 - (Exam Topic 2)

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

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

Answer: C

Question #:414 - (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

Question #:415 - (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

Question #:416 - (Exam Topic 2)

Which of the following is MOST important to enable well-informed cybersecurity risk decisions?

- A. Determine and understand the risk rating of scenarios.
- B. Conduct risk assessment peer reviews.
- C. Identify roles and responsibilities for security controls.
- D. Engage a third party to perform a risk assessment.

Answer: A

Question #:417 - (Exam Topic 2)

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

Question #:418 - (Exam Topic 2)

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

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

Answer: D

Question #:419 - (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

Question #:420 - (Exam Topic 2)

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

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

Answer: B

Question #:421 - (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: D

Question #:422 - (Exam Topic 2)

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

- A. Prepare a report for senior management.
- B. Assign responsibility and accountability for the incident.

- C. Update the risk register.
- D. Avoid recurrence of the incident.

Answer: D

Question #:423 - (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

Question #:424 - (Exam Topic 2)

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

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

Answer: B

Question #:425 - (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

Question #:426 - (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: B

Question #:427 - (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

Question #:428 - (Exam Topic 2)

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

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

Answer: D

Question #:429 - (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

Question #:430 - (Exam Topic 2)

An organization has initiated a project to implement an IT risk management program for the first time. The BEST time for the risk practitioner to start populating the risk register is when:

- A. identifying risk scenarios.
- B. determining the risk strategy.
- C. calculating impact and likelihood.
- D. completing the controls catalog.

Answer: A

Question #:431 - (Exam Topic 2)

Business areas within an organization have engaged various cloud service providers directly without assistance from the IT department. What should the risk practitioner do?

- A. Recommend the IT department remove access to the cloud services.
- B. Engage with the business area managers to review controls applied.
- C. Escalate to the risk committee.
- D. Recommend a risk assessment be conducted.

Answer: B

Question #:432 - (Exam Topic 2)

An internal audit report reveals that not all IT application databases have encryption in place. Which of the

following information would be MOST important for assessing the risk impact?

- A. The number of users who can access sensitive data
- B. A list of unencrypted databases which contain sensitive data
- C. The reason some databases have not been encrypted
- D. The cost required to enforce encryption

Answer: B

Question #:433 - (Exam Topic 2)

The FIRST task when developing a business continuity plan should be to:

- A. determine data backup and recovery availability at an alternate site.
- B. identify critical business functions and resources.
- C. define roles and responsibilities for implementation.
- D. identify recovery time objectives (RTOs) for critical business applications.

Answer: B

Question #:434 - (Exam Topic 2)

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

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

Answer: A

Question #:435 - (Exam Topic 2)

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

Question #:436 - (Exam Topic 2)

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

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

Answer: A

Question #:437 - (Exam Topic 2)

An organization has identified that terminated employee accounts are not disabled or deleted within the time required by corporate policy. Unsure of the reason, the organization has decided to monitor the situation for three months to obtain more information. As a result of this decision, the risk has been:

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

Answer: B

Question #:438 - (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

Question #:439 - (Exam Topic 2)

Which of the following is MOST helpful in aligning IT risk with business objectives?

- A. Introducing an approved IT governance framework
- B. Integrating the results of top-down risk scenario analyses
- C. Performing a business impact analysis (BlA)
- D. Implementing a risk classification system

Answer: A

Question #:440 - (Exam Topic 2)

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

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

Answer: A

Ouestion #:441 - (Exam Topic 2)

An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?

- A. Classification of the data
- B. Type of device
- C. Remote management capabilities
- D. Volume of data

Answer: A

Question #:442 - (Exam Topic 2)

An organization has implemented a system capable of comprehensive employee monitoring. Which of the following should direct how the system is used?

- A. Organizational strategy
- B. Employee code of conduct
- C. Industry best practices
- D. Organizational policy

Answer: D

Question #:443 - (Exam Topic 2)

Who is PRIMARILY accountable for risk treatment decisions?

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

Answer: B

Question #:444 - (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

Ouestion #:445 - (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

Question #:446 - (Exam Topic 2)

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

Question #:447 - (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

Question #:448 - (Exam Topic 2)

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

- A. The administrative access does not allow for activity log monitoring.
- B. The administrative access does not follow password management protocols.

- C. The administrative access represents a deviation from corporate policy.
- D. The administrative access represents a segregation of duties conflict.

Answer: D

Question #:449 - (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

Question #:450 - (Exam Topic 2)

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

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

Answer: B

Ouestion #:451 - (Exam Topic 2)

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

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

D. Potential impact of events

Answer: D

Question #:452 - (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

Question #:453 - (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: C

Question #:454 - (Exam Topic 2)

The PRIMARY goal of a risk management program is to:

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

Answer: B

Question #:455 - (Exam Topic 2)

Which of the following approaches would BEST help to identify relevant risk scenarios?

- A. Engage line management in risk assessment workshops.
- B. Escalate the situation to risk leadership.
- C. Engage internal audit for risk assessment workshops.
- D. Review system and process documentation.

Answer: A

Question #:456 - (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

Question #:457 - (Exam Topic 2)

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

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

Answer: A

Question #:458 - (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

Question #:459 - (Exam Topic 2)

Which of the following conditions presents the GREATEST risk to an application?

- A. Application controls are manual.
- B. Application development is outsourced.
- C. Source code is escrowed.
- D. Developers have access to production environment.

Answer: D

Question #:460 - (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: A

Question #:461 - (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

Question #:462 - (Exam Topic 2)

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

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

Answer: B

Question #:463 - (Exam Topic 2)

Which of the following is the PRIMARY benefit of identifying and communicating with stakeholders at the onset of an IT risk assessment?

- A. Obtaining funding support
- B. Defining the risk assessment scope
- C. Selecting the risk assessment framework
- D. Establishing inherent risk

Answer: B

Question #:464 - (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

Question #:465 - (Exam Topic 2)

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

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

Answer: B

Question #:466 - (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

About dumpscollection.com

<u>dumpscollection.com</u> was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors











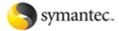














We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

Sales: sales@dumpscollection.com

Feedback: feedback@dumpscollection.comSupport: support@dumpscollection.com

Skype ID: <u>crack4sure@gmail.com</u>

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.

15% Discount Coupon Code:

DC15disc