Vendor: Isaca

Exam Code: CRISC

Exam Name: Certified in Risk and Information Systems Control

Version: DEMO

QUESTION 1
In addition to the risk exposure, which of the following is MOST important for senior management to understand prior to approving the use of artificial intelligence (AI) solutions?

A. Potential benefits from use of AI solutions
B. Monitoring techniques required for AI solutions
C. Changes to existing infrastructure to support AI solutions
D. Skills required to support AI solutions

Answer: A

QUESTION 2
Which of the following is MOST useful when performing a quantitative risk assessment?

A. RACI matrix
B. Financial models
C. Management support
D. Industry benchmarking

Answer: B

QUESTION 3
When determining risk ownership, the MAIN consideration should be:

A. who owns the business process.
B. the amount of residual risk.
C. who is responsible for risk mitigation.
D. the total cost of risk treatment.

Answer: A

QUESTION 4
The BEST way to mitigate the high cost of retrieving electronic evidence associated with potential litigation is to implement policies and procedures for:

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

Answer: C

QUESTION 5
To help ensure the success of a major IT project, it is MOST important to:

A. obtain the appropriate stakeholders' commitment.
B. align the project with the IT risk framework.
C. obtain approval from business process owners.
D. update the risk register on a regular basis.

Answer: A

QUESTION 6
Which of the following is the PRIMARY reason to conduct risk assessments at periodic intervals?

A. To ensure emerging risk is identified and monitored
B. To establish the maturity level of risk assessment processes
C. To promote a risk-aware culture among staff
D. To ensure risk trend data is collected and reported

Answer: A

QUESTION 7
Which of the following provides the MOST mitigation value for an organization implementing new Internet of Things (IoT) devices?

A. Performing a vulnerability assessment on the IoT devices
B. Designing IoT architecture with IT security controls from the start
C. Implementing key risk indicators (KRIs) for IoT devices
D. To ensure risk trend data is collected and reported

Answer: B

QUESTION 8
Which of the following is the MOST critical consideration when awarding a project to a third-party service provider whose servers are located offshore?

A. Difficulty of monitoring compliance due to geographical distance
B. Cost implications due to installation of network intrusion detection systems (IDSs)
C. Delays in incident communication
D. Potential impact on data governance

Answer: D

QUESTION 9
A new risk practitioner finds that decisions for implementing risk response plans are not being made. Which of the following would MOST likely explain this situation?

A. Risk ownership is not being assigned properly.
B. The organization has a high level of risk appetite.
C. Risk management procedures are outdated.
D. The organization's risk awareness program is ineffective.

Answer: A

QUESTION 10
A recently purchased IT application does not meet project requirements. Of the following, who is

accountable for the potential impact?

A. Business analyst
B. Project sponsor
C. IT project team
D. IT project management office (PMO)

Answer: B

QUESTION 11
A risk practitioner finds that data has been misclassified. Which of the following is the GREATEST concern?

A. Unauthorized access
B. Data corruption
C. Inadequate retention schedules
D. Data disruption

Answer: A

QUESTION 12
An organization has outsourced its customer management database to an external service provider. Of the following, who should be accountable for ensuring customer data privacy?

A. The organization's business process owner
B. The organization's information security manager
C. The organization's vendor management officer
D. The vendor's risk manager

Answer: A

QUESTION 13
Following the implementation of an Internet of Things (IoT) solution, a risk practitioner identifies new risk factors with impact to existing controls. Which of the following is MOST important to include in a report to stakeholders?

A. Identified vulnerabilities
B. Business managers' concerns
C. Changes to residual risk
D. Risk strategies of peer organizations

Answer: C

QUESTION 14
Which of the following should a risk practitioner review FIRST when evaluating risk events associated with the organization's data flow model?

A. Results of data classification activities
B. Recent changes to enterprise architecture (EA)

C. High-level network diagrams
D. Notes from interviews with the data owners

Answer: A

QUESTION 15
Which of the following controls will BEST mitigate risk associated with excessive access privileges?

A. Review of user access logs
B. Frequent password expiration
C. Separation of duties
D. Entitlement reviews

Answer: D

QUESTION 16
A technology company is developing a strategic artificial intelligence (AI)-driven application that has high potential business value. At what point should the enterprise risk profile be updated?

A. After user acceptance testing (UAT)
B. Upon approval of the business case
C. When user stories are developed
D. During post-implementation review

Answer: B

QUESTION 17
Which of the following is a risk practitioner's BEST course of action if a risk assessment identifies a risk that is extremely unlikely but would have a severe impact should it occur?

A. Rate the risk as high priority based on the severe impact.
B. Obtain management's consent to accept the risk.
C. Ignore the risk due to the extremely low likelihood.
D. Address the risk by analyzing treatment options.

Answer: D

QUESTION 18
Which of the following should be done FIRST when developing an initial set of risk scenarios for an organization?

A. Refer to industry standard scenarios.
B. Use a top-down approach.
C. Consider relevant business activities.
D. Use a bottom-up approach.

Answer: C

QUESTION 19
Which of the following is MOST important for a risk practitioner to understand about an organization in order to create an effective risk
awareness program?

A. Policies and procedures
B. Structure and culture
C. Key risk indicators (KRIs) and thresholds
D. Known threats and vulnerabilities

Answer: D

QUESTION 20
Which of the following is the PRIMARY advantage of having a single integrated business continuity plan (BCP) rather than each business unit developing its own BCP?

A. It provides assurance of timely business process response and effectiveness.
B. It supports effective use of resources and provides reasonable confidence of recoverability.
C. It enables effective BCP maintenance and updates to reflect organizational changes.
D. It decreases the risk of downtime and operational losses in the event of a disruption.

Answer: C

QUESTION 21
An organization is implementing Zero Trust architecture to improve its security posture. Which of the following is the MOST important input to develop the architecture?

A. Cloud services risk assessments
B. The organization's threat model
C. Access control logs
D. Multi-factor authentication (MFA) architecture

Answer: B

QUESTION 22
Who is PRIMARILY accountable for identifying risk on a daily basis and ensuring adherence to the organization's policies?

A. Third line of defense
B. Line of defense subject matter experts
C. Second line of defense
D. First line of defense

Answer: D

QUESTION 23
Which of the following is the PRIMARY risk management responsibility of the third line of defense?

A. Providing assurance of the effectiveness of risk management activities
B. Providing guidance on the design of effective controls
C. Providing advisory services on enterprise risk management (ERM)
D. Providing benchmarking on other organizations' risk management programs

Answer: A

QUESTION 24
Which of the following is a PRIMARY objective of privacy impact assessments (PIAs)?

A. To identify threats introduced by business processes
B. To identify risk when personal information is collected
C. To ensure senior management has approved the use of personal information
D. To ensure compliance with data privacy laws and regulations

Answer: D

QUESTION 25
Within the risk management space, which of the following activities could be delegated to a cloud service provider?

A. Risk oversight
B. Control implementation
C. Incident response
D. User access reviews

Answer: B

QUESTION 26
External penetration tests MUST include:

A. use of consultants to ensure completeness.
B. communications to users of the target systems.
C. changes to target data to prove the attack was successful.
D. advance approval from system owners.

Answer: D

QUESTION 27
A business unit has implemented robotic process automation (RPA) for its repetitive back-office tasks. Which of the following should be the risk practitioner's GREATEST concern?

A. The security team is unaware of the implementation.
B. The organization may lose institutional knowledge.
C. The robots may fail to work effectively.
D. Virtual clients are used for implementation.

Answer: A

QUESTION 28
Senior management has requested a risk practitioner's guidance on whether a new technical control requested by a business unit is worth the investment. Which of the following should be the MOST important consideration before providing input?

A. The cost of the control relative to the value of risk mitigation
B. The effectiveness of the control at reducing residual risk levels
C. The likelihood of a successful attack based on current risk
D. assessments
E. The availabilitv of budgeted funds for risk mitigationMitination

Answer: B

QUESTION 29
A new international data privacy regulation requires personal data to be disposed after the specified retention period, which is different from the local regulatory requirement. Which of the following is the risk practitioner's BEST course of action?

A. The application code has not been version controlled.
B. Knowledge of the applications is limited to few employees.
C. An IT project manager is not assigned to oversee development.
D. Controls are not applied to the applications.

Answer: D

QUESTION 30
Which of the following presents the GREATEST concern associated with the use of artificial intelligence (AI) systems?

A. AI systems need to be available continuously.
B. AI systems can be affected by bias.
C. AI systems are expensive to maintain.
D. AI systems can provide false positives.

Answer: B

QUESTION 31
An organization has determined that risk is not being adequately tracked and managed due to a distributed operating model. Which of the following is the BEST way to address this issue?

A. Increase the frequency of risk assessments.
B. Revalidate the organization's risk appetite
C. Create a centralized portfolio of risk scenarios.
D. Create dashboards for risk metrics.

Answer: C

QUESTION 32
Upon learning that the number of failed backup attempts continually exceeds the current risk threshold, the risk practitioner should:

A. initiate corrective action to address the known deficiency.
B. adjust the risk threshold to better reflect actual performance.
C. inquire about the status of any planned corrective actions.
D. keep monitoring the situation as there is evidence that this is normal.

Answer: A

QUESTION 33
Which of the following BEST indicates that an organization's disaster recovery plan (DRP) will mitigate the risk of the organization failing to recover from a major service disruption?

A. A defined recovery point objective (RPO)
B. An experienced and certified disaster recovery team
C. A comprehensive list of critical applications
D. A record of quarterly disaster recovery tests

Answer: A

QUESTION 34
Which of the following BEST helps to ensure disaster recovery staff members are able to complete their assigned tasks effectively during a disaster?

A. Performing parallel disaster recovery testing
B. Documenting the order of system and application restoration
C. Involving disaster recovery staff members in risk assessments
D. Conducting regular tabletop exercises and scenario analysis

Answer: D

QUESTION 35
An organization becomes aware that IT security failed to detect a coordinated cyber attack on its data center. Which of the following is the BEST course of action?

A. Perform a business impact analysis (BIA).
B. Identify compensating controls
C. Conduct a root cause analysis.
D. Revise key risk indicator (KRI) thresholds.

Answer: C

QUESTION 36
Which of the following is the PRIMARY purpose of a risk register?

A. It guides management in determining risk appetite.
B. It provides management with a risk inventory.

C. It aligns risk scenarios to business objectives.
D. It monitors the performance of risk and control owners.

Answer: B

QUESTION 37
Who is accountable for the process when an IT stakeholder operates a key control to address a risk scenario?

A. Risk owner
B. IT manager
C. System owner
D. Data custodian

Answer: A

QUESTION 38
Which of the following BEST facilitates the identification of emerging risk?

A. Performing scenario-based assessments
B. Reviewing audit reports annually
C. Conducting root cause analyses
D. Engaging a risk-focused audit team

Answer: A

QUESTION 39
Which of the following BEST enables effective risk reporting to the board of directors?

A. Presenting case studies of breaches from other similar organizations
B. Mapping risk scenarios to findings identified by internal audit
C. Communicating in terms that correlate to corporate objectives and business value
D. Reporting key metrics that indicate the efficiency and effectiveness of risk governance

Answer: C

QUESTION 40
The patch management process is MOST effectively monitored through which of the following key control indicators (KCIs)?

A. Number of legacy servers out of support
B. Percentage of patches deployed within the target time frame
C. Number of patches deployed outside of business hours
D. Percentage of patched systems tested

Answer: B