Isaca

Exam Questions CRISC

Certified in Risk and Information Systems Control

NEW QUESTION 1
- (Exam Topic 4)
Which of the following would provide the MOST reliable evidence of the effectiveness of security controls implemented for a web application?

A. Penetration testing
B. IT general controls audit
C. Vulnerability assessment
D. Fault tree analysis

Answer: A

NEW QUESTION 2
- (Exam Topic 4)
Which of the following presents the GREATEST challenge to managing an organization's end-user devices?

A. Incomplete end-user device inventory
B. Unsupported end-user applications
C. Incompatible end-user devices
D. Multiple end-user device models

Answer: A

NEW QUESTION 3
- (Exam Topic 4)
A recent big data project has resulted in the creation of an application used to support important investment decisions. Which of the following should be of GREATEST concern to the risk practitioner?

A. Data quality
B. Maintenance costs
C. Data redundancy
D. System integration

Answer: A

NEW QUESTION 4
- (Exam Topic 3)
Which of the following should be the FIRST consideration when a business unit wants to use personal information for a purpose other than for which it was originally collected?

A. Informed consent
B. Cross border controls
C. Business impact analysis (BIA)
D. Data breach protection

Answer: A

NEW QUESTION 5
- (Exam Topic 3)
Which of the following is MOST important when developing key risk indicators (KRIs)?

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

Answer: C

NEW QUESTION 6
- (Exam Topic 3)
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

NEW QUESTION 7
- (Exam Topic 3)
Print jobs containing confidential information are sent to a shared network printer located in a secure room. Which of the following is the BEST control to prevent the inappropriate disclosure of confidential information?

A. Requiring a printer access code for each user
B. Using physical controls to access the printer room

C. Using video surveillance in the printer room
D. Ensuring printer parameters are properly configured

Answer: A

NEW QUESTION 8
- (Exam Topic 4)
As pan of business continuity planning, which of the following is MOST important to include m a business impact analysis (BlA)?

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

Answer: A

NEW QUESTION 9
- (Exam Topic 4)
An organization retains footage from its data center security camera for 30 days when the policy requires 90-day retention The business owner challenges whether the situation is worth remediating Which of the following is the risk manager s BEST response'

A. Identify the regulatory bodies that may highlight this gap
B. Highlight news articles about data breaches
C. Evaluate the risk as a measure of probable loss
D. Verify if competitors comply with a similar policy

Answer: B

NEW QUESTION 10
- (Exam Topic 4)
An organization has made a decision to purchase a new IT system. During when phase of the system development life cycle (SDLC) will identified risk MOST likely lead to architecture and design trade-offs?

A. Acquisition
B. Implementation
C. Initiation
D. Operation and maintenance

Answer: C

NEW QUESTION 11
- (Exam Topic 4)
Which of the following is the PRIMARY reason to perform periodic vendor risk assessments?

A. To provide input to the organization's risk appetite
B. To monitor the vendor's control effectiveness
C. To verify the vendor's ongoing financial viability
D. To assess the vendor's risk mitigation plans

Answer: B

NEW QUESTION 12
- (Exam Topic 4)
Which of the following is the PRIMARY benefit of stakeholder involvement in risk scenario development?

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

Answer: A

NEW QUESTION 13
- (Exam Topic 4)
Which of the following is the BEST course of action when an organization wants to reduce likelihood in order to reduce a risk level?

A. Monitor risk controls.
B. Implement preventive measures.
C. Implement detective controls.
D. Transfer the risk.

Answer: B

NEW QUESTION 14
- (Exam Topic 4)

Who should be responsible for determining which stakeholders need to be involved in the development of a risk scenario?

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

Answer: B

NEW QUESTION 15
- (Exam Topic 4)
Which of the following would BEST mitigate the ongoing risk associated with operating system (OS) vulnerabilities?

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

Answer: B

NEW QUESTION 16
- (Exam Topic 3)
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

NEW QUESTION 17
- (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: A

NEW QUESTION 18
- (Exam Topic 2)
Which of the following could BEST detect an in-house developer inserting malicious functions into a web-based application?

A. Segregation of duties
B. Code review
C. Change management
D. Audit modules

Answer: B

NEW QUESTION 19
- (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

NEW QUESTION 20
- (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

NEW QUESTION 21
- (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

NEW QUESTION 22
- (Exam Topic 2)
Which of the following BEST contributes to the implementation of an effective risk response action plan?

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

Answer: C

NEW QUESTION 23
- (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

NEW QUESTION 24
- (Exam Topic 2)
Of the following, who should be responsible for determining the inherent risk rating of an application?

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

Answer: C

NEW QUESTION 25
- (Exam Topic 1)
Which of the following will BEST help mitigate the risk associated with malicious functionality in outsourced application development?

A. Perform an m-depth code review with an expert
B. Validate functionality by running in a test environment
C. Implement a service level agreement.
D. Utilize the change management process.

Answer: C

NEW QUESTION 26
- (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

NEW QUESTION 27
- (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

NEW QUESTION 28
- (Exam Topic 1)
An organization has identified a risk exposure due to weak technical controls in a newly implemented HR system. The risk practitioner is documenting the risk in the risk register. The risk should be owned by the:

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

Answer: D

NEW QUESTION 29
- (Exam Topic 1)
An organization has allowed its cyber risk insurance to lapse while seeking a new insurance provider. The risk practitioner should report to management that the risk has been:

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

Answer: C

NEW QUESTION 30
- (Exam Topic 1)
The PRIMARY reason a risk practitioner would be interested in an internal audit report is to:

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

Answer: C

NEW QUESTION 31
......