ISACA

CRISC

Certified in Risk and

Information Systems Control

ISACA

Exam CRISC

Certified in Risk and Information Systems Control

Version: 21.0

[Total Questions: 1197]

Topic break down

Topic	No. of Questions
Topic 1: Exam Pool A	167
Topic 2: Exam Pool B	371
Topic 3: Exam Pool C	355
Topic 4: Exam Pool D	304

Topic 1, Exam Pool A

Question No : 1 - (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 No : 2 - (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

Question No : 3 - (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: C

Question No : 4 - (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 No : 5 - (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 No : 6 - (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 No : 7 - (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 No : 8 - (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 No : 9 - (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 No : 10 - (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

Question No : 11 - (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 No : 12 - (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 No : 13 - (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 No : 14 - (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 No : 15 - (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 No : 16 - (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: C

Question No : 17 - (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 No : 18 - (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 No : 19 - (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 No : 20 - (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 No : 21 - (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 No : 22 - (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 No : 23 - (Topic 1)

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

management would be to:

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

Answer: A

Question No : 24 - (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 No : 25 - (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 No : 26 - (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 No : 27 - (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 No : 28 - (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 No : 29 - (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 No : 30 - (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 No : 31 - (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 No : 32 - (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

Question No : 33 - (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 No : 34 - (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 No : 35 - (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 No : 36 - (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 No : 37 - (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 No : 38 - (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 No : 39 - (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 No : 40 - (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 No : 41 - (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 No : 42 - (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 No : 43 - (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 No : 44 - (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 No : 45 - (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 No : 46 - (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: B

Question No : 47 - (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 No : 48 - (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 No : 49 - (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 No : 50 - (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 No : 51 - (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 No : 52 - (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 No : 53 - (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 No : 54 - (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 No : 55 - (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 No : 56 - (Topic 1)