Isaca

Exam Questions IT-Risk-Fundamentals

IT Risk Fundamentals CertificateExam

NEW QUESTION 1
Which of the following is an example of an inductive method to gather information?

A. Vulnerability analysis
B. Controls gap analysis
C. Penetration testing

Answer: C

NEW QUESTION 2
An enterprise??s risk policy should be aligned with its:

A. current risk.
B. risk capacity.
C. risk appetite.

Answer: C

NEW QUESTION 3
Which of the following is a benefit of using a top-down approach when developing risk scenarios?

A. Focus at the enterprise level makes it easier to achieve management support.
B. The development process is simplified because it includes only I&T-related events.
C. Identification and assignment of risk ownership for mitigation plans can be done more quickly.

Answer: A

NEW QUESTION 4
Incomplete or inaccurate data may result in:

A. availability risk.
B. relevance risk.
C. integrity risk.

Answer: C

NEW QUESTION 5
The MOST important reason to monitor implemented controls is to ensure the controls:

A. are effective and manage risk to the desired level.
B. enable IT operations to meet agreed service levels.
C. mitigate risk associated with regulatory noncompliance.

Answer: A

NEW QUESTION 6
When determining the criticality of I&T assets, it is MOST important to identify:

A. the asset owners who are accountable for asset valuation.
B. the business processes in which the asset is used to achieve objectives.
C. the infrastructure in which the asset is processed and stored.

Answer: B

NEW QUESTION 7
When selecting a key risk indicator (KRI), it is MOST important that the KRI:

A. supports established KPIs.
B. produces multiple and varied results.
C. is a reliable predictor of the risk event.

Answer: C

NEW QUESTION 8
Which of the following occurs earliest in the risk response process?

A. Developing risk response plans
B. Prioritizing risk responses
C. Analyzing risk response options

Answer: C

NEW QUESTION 9
Which of the following is the MAIN objective of governance?

A. Creating controls throughout the entire organization
B. Creating risk awareness at all levels of the organization
C. Creating value through investments for the organization

Answer: C

NEW QUESTION 10
Which of the following are KEY considerations when selecting the best risk response for a given situation?

A. Alignment with risk policy and industry standards
B. Previous risk response strategies and action plans
C. Cost of the response and capability to implement

Answer: C

NEW QUESTION 10
Which of the following includes potential risk events and the associated impact?

A. Risk scenario
B. Risk policy
C. Risk profile

Answer: A

NEW QUESTION 13
Which of the following is important to ensure when validating the results of a frequency analysis?

A. Estimates used during the analysis were based on reliable and historical data.
B. The analysis was conducted by an independent third party.
C. The analysis method has been fully documented and explained.

Answer: A

NEW QUESTION 15
Which of the following is the FIRST step in an advanced persistent threat (APT) attack?

A. Identify administrators and crack passwords to obtain administrator access.
B. Use social engineering to encourage employees to visit an infected website.
C. Collect information on the infrastructure of an organization to know where to attack.

Answer: C

NEW QUESTION 17
Which of the following statements on an organization's cybersecurity profile is BEST suited for presentation to management?

A. The probability of a cyber attack varies between unlikely and very likely.
B. Risk management believes the likelihood of a cyber attack is not imminent.
C. Security measures are configured to minimize the risk of a cyber attack.

Answer: C

NEW QUESTION 18
As part of an I&T related risk assessment, which of the following should be reviewed to obtain an initial view of overall I&T related risk for the enterprise?

A. Threats and vulnerabilities for each risk factor identified
B. Components of the risk register with remediation plans
C. Components of the risk universe at a high level

Answer: C

NEW QUESTION 22
Risk impact criteria are PRIMARILY used to:

A. help establish the enterprise risk appetite.
B. determine loss associated with specific IT assets.
C. prioritize the enterprise's risk responses.

Answer: C

NEW QUESTION 23
Which of the following should be found in an I&T asset inventory to help inform the risk identification process?

A. Loss scenario information for assets
B. Security classification of assets
C. Regulatory requirements of assets

Answer: B

NEW QUESTION 28
Which of the following is the BEST way to interpret enterprise standards?

A. A means of implementing policy
B. An approved code of practiceQ Documented high-level principles

Answer: A

NEW QUESTION 29
Which of the following is the PRIMARY reason for an organization to monitor and review I&T-related risk periodically?

A. To address changes in external and internal risk factors
B. To ensure risk is managed within acceptable limits
C. To facilitate the timely identification and replacement of legacy IT assets

Answer: A

NEW QUESTION 32
Which of the following is the MOST important information for determining the critical path of a project?

A. Regulatory requirements
B. Cost-benefit analysis
C. Specified end dates

Answer: C

NEW QUESTION 35
Which type of assessment evaluates the changes in technical or operating environments that could result in adverse consequences to an enterprise?

A. Vulnerability assessment
B. Threat assessment
C. Control self-assessment

Answer: B

NEW QUESTION 37
Which of the following is combined with risk impact to determine the level of risk?

A. Threat level
B. Likelihood
C. Vulnerability score

Answer: B

NEW QUESTION 41
To be effective, risk reporting and communication should provide:

A. risk reports to each business unit and groups of employees.
B. the same risk information for each decision-making stakeholder.
C. stakeholders with concise information focused on key points.

Answer: C

NEW QUESTION 43
An enterprise has performed a risk assessment for the risk associated with the theft of sales team laptops while in transit. The results of the assessment concluded that the cost of mitigating the risk is higher than the potential loss. Which of the following is the BEST risk response strategy?

A. Limit travel with laptops.
B. Accept the inherent risk.
C. Encrypt the sales team laptops.

Answer: B

NEW QUESTION 46
Which of the following is a KEY contributing component for determining risk rankings to direct risk response?

A. Cost of mitigating controls
B. Severity of a vulnerability

C. Maturity of risk management processes

Answer: A

NEW QUESTION 47
Which of the following MUST be established in order to manage l&T-related risk throughout the enterprise?

A. An enterprise risk governance committee
B. The enterprise risk universe
C. Industry best practices for risk management

Answer: A

NEW QUESTION 49
Key risk indicators (KRIs) are metrics designed to:

A. alert there is an increased chance of exceeding risk appetite.
B. be a direct measure of risk for each business line.
C. measure current risk levels in comparison to past levels.

Answer: A

NEW QUESTION 50
Which of the following would be considered a cyber-risk?

A. A system that does not meet the needs of users
B. A change in security technology
C. Unauthorized use of information

Answer: C

NEW QUESTION 53
An enterprise recently implemented multi-factor authentication. During the most recent risk assessment, it was determined that cybersecurity risk is within the organization's risk appetite threshold. What is the MOST appropriate action for the organization to take regarding the remaining cybersecurity residual risk?

A. Accept
B. Mitigate
C. Transfer

Answer: A

NEW QUESTION 58
The PRIMARY reason for the implementation of additional security controls is to:

A. avoid the risk of regulatory noncompliance.
B. adhere to local data protection laws.
C. manage risk to acceptable tolerance levels.

Answer: C

NEW QUESTION 63
Which of the following is MOST important when defining an organization's risk scope?

A. Understanding the impacts of the risk environment to the organization
B. Developing a top-down approach to risk management
C. Developing requirements for risk reporting to executive management

Answer: A

NEW QUESTION 67
Which of the following is the MOST likely reason to perform a qualitative risk analysis?

A. To gain a low-cost understanding of business unit dependencies and interactions
B. To aggregate risk in a meaningful way for a comprehensive view of enterprise risk
C. To map the value of benefits that can be directly compared to the cost of a risk response

Answer: A

NEW QUESTION 70
What is the purpose of a control objective?

A. To describe the result of protecting an asset for a business process
B. To describe the risk of loss to an asset
C. To describe the responsibility of stakeholders to protect assets

Answer: A

NEW QUESTION 72
Which of the following is MOST important to include when developing a business case for a specific risk response?

A. Stakeholders responsible for the risk response plan
B. Communication and status reporting of the related risk
C. A justification for the expense of the investment

Answer: C

NEW QUESTION 73
Which of the following is considered an exploit event?

A. An attacker takes advantage of a vulnerability
B. Any event that is verified as a security breach
C. The actual occurrence of an adverse event

Answer: A

NEW QUESTION 74
Which of the following MUST be consistent with the defined criteria when establishing the risk management context as it relates to calculation of risk?

A. Risk appetite and tolerance levels
B. Formulas and methods for combining impact and likelihood
C. Key risk indicators (KRIs) and key performance indicators (KPIs)

Answer: B

NEW QUESTION 77
Which of the following is the PRIMARY concern with vulnerability assessments?

A. Threat mitigation
B. Report size
C. False positives

Answer: C

NEW QUESTION 80
Which risk response option has been adopted when an enterprise outsources disaster recovery activities to leverage the skills and expertise of a third-party provider?

A. Risk mitigation
B. Risk avoidance
C. Risk transfer

Answer: C

NEW QUESTION 84
Which of the following is the MAIN reason to conduct a penetration test?

A. To validate the results of a vulnerability assessment
B. To validate the results of a control self-assessment
C. To validate the results of a threat assessment

Answer: A

NEW QUESTION 88
Of the following, who is BEST suited to be responsible for continuous monitoring of risk?

A. Chief risk officer (CRO)
B. Risk analysts
C. Risk owners

Answer: C

NEW QUESTION 91
When should a consistent risk analysis method be used?

A. When the goal is to produce results that can be compared over time
B. When the goal is to aggregate risk at the enterprise level
C. When the goal is to prioritize risk response plans

Answer: A

NEW QUESTION 92
Organizations monitor control statuses to provide assurance that:

A. compliance with established standards is achieved.
B. risk events are being fully mitigated.
C. return on investment (ROI) objectives are met.

Answer: A

NEW QUESTION 97
Why is risk identification important to an organization?

A. It provides a review of previous and likely threats to the enterprise.
B. It ensures risk is recognized and the impact to business objectives is understood.
C. It enables the risk register to detail potential impacts to an enterprise's business processes.

Answer: B

NEW QUESTION 101
Applying statistical analysis methods to I&T risk scenarios is MOST appropriate when:

A. quantifiable historical data is available for detailed reviews.
B. risk management professionals are unfamiliar with qualitative methods.
C. members of senior management have advanced mathematical knowledge.

Answer: A

NEW QUESTION 106
The MOST important reason for developing and monitoring key risk indicators (KRIs) is that they provide:

A. measurable metrics for acceptable risk levels.
B. information about control compliance.
C. an early warning of possible risk materialization.

Answer: C

NEW QUESTION 111
Which of the following is of GREATEST concern when aggregating risk information in management reports?

A. Duplicating details of risk status
B. Obfuscating the reasons behind risk
C. Generalizing acceptable risk levels

Answer: B

NEW QUESTION 116
A key risk indicator (KRI) is PRIMARILY used for which of the following purposes?

A. Optimizing risk management
B. Predicting risk events
C. Facilitating dashboard reporting

Answer: B

NEW QUESTION 121
Which of the following provides the BEST input when developing specific, measurable, realistic, and time-bound (SMART) metrics?

A. Associated business functions or services
B. Industry best practices
C. Enterprise risk management strategy

Answer: A

NEW QUESTION 124
Which of the following BEST supports a risk-aware culture within an enterprise?

A. Risk issues and negative outcomes are only shared within a department.
B. The enterprise risk management (ERM) function manages all risk-related activities.
C. Risk is identified, documented, and discussed to make business decisions.

Answer: C

NEW QUESTION 129

An enterprise has moved its data center from a flood-prone area where it had experienced significant service disruptions to one that is not a flood zone. Which risk response strategy has the organization selected?

A. Risk mitigation
B. Risk transfer
C. Risk avoidance

Answer: C

NEW QUESTION 133
......