Vendor: Isaca

Exam Code: CRISC

Exam Name: Certified in Risk and Information Systems Control

Version: DEMO

QUESTION 1

Which of the following events refer to loss of integrity?
Each correct answer represents a complete solution. Choose three.

A. Someone sees company's secret formula
B. Someone makes unauthorized changes to a Web site
C. An e-mail message is modified in transit
D. A virus infects a file

Answer: BCD
Explanation:
Loss of integrity refers to the following types of losses:

- An e-mail message is modified in transit A virus infects a file
- Someone makes unauthorized changes to a Web site

Incorrect Answers:
A: Someone sees company's secret formula or password comes under loss of confidentiality.

QUESTION 2

Which of the following should be PRIMARILY considered while designing information systems controls?

A. The IT strategic plan
B. The existing IT environment
C. The organizational strategic plan
D. The present IT budget

Answer: C
Explanation:
Review of the enterprise's strategic plan is the first step in designing effective IS controls that would fit the enterprise's long-term plans.
Incorrect Answers:
A: The IT strategic plan exists to support the enterprise's strategic plan but is not solely considered while designing information system control.
B: Review of the existing IT environment is also useful and necessary but is not the first step that needs to be undertaken.
D: The present IT budget is just one of the components of the strategic plan.

QUESTION 3

Which of the following is the MOST effective inhibitor of relevant and efficient communication?

A. A false sense of confidence at the top on the degree of actual exposure related to IT and lack of a well- understood direction for risk management from the top down
B. The perception that the enterprise is trying to cover up known risk from stakeholders
C. Existence of a blame culture
D. Misalignment between real risk appetite and translation into policies

Answer: C
Explanation:
Blame culture should be avoided. It is the most effective inhibitor of relevant and efficient communication.
In a blame culture, business units tend to point the finger at IT when projects are not delivered on

time or do not meet expectations. In doing so, they fail to realize how the business unit's involvement up front affects project success. In extreme cases, the business unit may assign blame for a failure to meet the expectations that the unit never clearly communicated. Executive leadership must identify and quickly control a blame culture if collaboration is to be fostered throughout the enterprise.
Incorrect Answers:
A: This is the consequence of poor risk communication, not the inhibitor of effective communication.
B: This is the consequence of poor risk communication, not the inhibitor of effective communication.
D: Misalignment between real risk appetite and translation into policies is an inhibitor of effective communication, but is not a prominent as existence of blame culture.

QUESTION 4
You and your project team are identifying the risks that may exist within your project. Some of the risks are small risks that won't affect your project much if they happen. What should you do with these identified risk events?

A. These risks can be dismissed.
B. These risks can be accepted.
C. These risks can be added to a low priority risk watch list.
D. All risks must have a valid, documented risk response.

Answer: C
Explanation:
Low-impact, low-probability risks can be added to the low priority risk watch list.
Incorrect Answers:
A: These risks are not dismissed; they are still documented on the low priority risk watch list.
B: While these risks may be accepted, they should be documented on the low priority risk watch list. This list will be periodically reviewed and the status of the risks may change.
D: Not every risk demands a risk response, so this choice is incorrect.

QUESTION 5
You are the project manager of your enterprise. You have introduced an intrusion detection system for the control. You have identified a warning of violation of security policies of your enterprise. What type of control is an intrusion detection system (IDS)?

A. Detective
B. Corrective
C. Preventative
D. Recovery

Answer: A
Explanation:
An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.
Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. As IDS detects and gives warning when the violation of security policies of the enterprise occurs,

it is a detective control.
Incorrect Answers:
B: These controls make effort to reduce the impact of a threat from problems discovered by detective controls. As IDS only detects but not reduce the impact, hence it is not a corrective control.
C: As IDS only detects the problem when it occurs and not prior of its occurrence, it is not preventive control.
D: These controls make efforts to overcome the impact of the incident on the business, hence IDS is not a recovery control.

QUESTION 6
What are the functions of audit and accountability control?

Each correct answer represents a complete solution. (Choose three.)

A. Provides details on how to protect the audit logs
B. Implement effective access control
C. Implement an effective audit program
D. Provides details on how to determine what to audit

Answer: ACD
Explanation:
Audit and accountability family of controls helps an organization implement an effective audit program. It provides details on how to determine what to audit. It provides details on how to protect the audit logs. It also includes information on using audit logs for non-repudiation.
Incorrect Answers:
B: Access Control is the family of controls that helps an organization implement effective access control.
They ensure that users have the rights and permissions they need to perform their jobs, and no more. It includes principles such as least privilege and separation of duties.
Audit and accountability family of controls do not help in implementing effective access control.

QUESTION 7
Which among the following acts as a trigger for risk response process?

A. Risk level increases above risk appetite
B. Risk level increase above risk tolerance
C. Risk level equates risk appetite
D. Risk level equates the risk tolerance

Answer: B
Explanation:
The risk response process is triggered when a risk exceeds the enterprise's risk tolerance level. The acceptable variation relative to the achievement of an objective is termed as risk tolerance. In other words, risk tolerance is the acceptable deviation from the level set by the risk appetite and business objectives.

Risk tolerance is defined at the enterprise level by the board and clearly communicated to all stakeholders. A process should be in place to review and approve any exceptions to such standards.

Incorrect Answers:
A, C: Risk appetite level is not relevant in triggering of risk response process. Risk appetite is the

amount of risk a company or other entity is willing to accept in pursuit of its mission. This is the responsibility of the board to decide risk appetite of an enterprise. When considering the risk appetite levels for the enterprise, the following two major factors should be taken into account:

- The enterprise's objective capacity to absorb loss, e.g., financial loss, reputation damage, etc.
- The culture towards risk taking-cautious or aggressive. In other words, the amount of loss the enterprise wants to accept in pursue of its objective fulfillment.

D: Risk response process is triggered when the risk level increases the risk tolerance level of the enterprise, and not when it just equates the risk tolerance level.

QUESTION 8
What is the value of exposure factor if the asset is lost completely?

A. 1
B. Infinity
C. 10
D. 0

Answer: A
Explanation:
Exposure Factor represents the impact of the risk over the asset, or percentage of asset lost. For example, if the Asset Value is reduced to two third, the exposure factor value is 0.66.
Therefore, when the asset is completely lost, the Exposure Factor is 1.0.
Incorrect Answers:
B, C, D: These are not the values of exposure factor for zero assets.

QUESTION 9
Your project is an agricultural-based project that deals with plant irrigation systems. You have discovered a byproduct in your project that your organization could use to make a profit. If your organization seizes this opportunity it would be an example of what risk response?

A. Enhancing
B. Positive
C. Opportunistic
D. Exploiting

Answer: D
Explanation:
This is an example of exploiting a positive risk - a by-product of a project is an excellent example of exploiting a risk. Exploit response is one of the strategies to negate risks or threats that appear in a project.
This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Exploiting a risk event provides opportunities for positive impact on a project.
Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.
Incorrect Answers:
A: Enhancing is a positive risk response that describes actions taken to increase the odds of a risk event to happen.
B: This is an example of a positive risk, but positive is not a risk response.
C: Opportunistic is not a valid risk response.

QUESTION 10

Which of the following is true for Single loss expectancy (SLE), Annual rate of occurrence (ARO), and Annual loss expectancy (ALE)?

A. ALE= ARO/SLE
B. ARO= SLE/ALE
C. ARO= ALE*SLE
D. ALE= ARO*SLE

Answer: D

Explanation:

A quantitative risk assessment quantifies risk in terms of numbers such as dollar values. This involves gathering data and then entering it into standard formulas. The results can help in identifying the priority of risks. These results are also used to determine the effectiveness of controls. Some of the terms associated with quantitative risk assessments are:

- Single loss expectancy (SLE)-It refers to the total loss expected from a single incident. This incident can occur when vulnerability is being exploited by threat. The loss is expressed as a dollar value such as $1,000. It includes the value of data, software, and hardware. SLE = Asset value * Exposure factor
- Annual rate of occurrence (ARO)-It refers to the number of times expected for an incident to occur in a year. If an incident occurred twice a month in the past year, the ARO is 24. Assuming nothing changes, it is likely that it will occur 24 times next year. Annual loss expectancy (ALE)-It is the expected loss for a year. ALE is calculated by multiplying SLE with ARO. Because SLE is a given in a dollar value, ALE is also given in a dollar value. For example, if the SLE is $1,000 and the ARO is 24, the ALE is $24,000.
- ALE = SLE * ARO Safeguard value-This is the cost of a control. Controls are used to mitigate risk. For example, antivirus software of an average cost of $50 for each computer. If there are 50 computers, the safeguard value is $2,500. A, B, C: These are wrong formulas and are not used in quantitative risk assessment.

QUESTION 11

Which of the following statements are true for enterprise's risk management capability maturity level 3?

A. Workflow tools are used to accelerate risk issues and track decisions
B. The business knows how IT fits in the enterprise risk universe and the risk portfolio view
C. The enterprise formally requires continuous improvement of risk management skills, based on clearly defined personal and enterprise goals
D. Risk management is viewed as a business issue, and both the drawbacks and benefits of risk are recognized

Answer: ABD

Explanation:

An enterprise's risk management capability maturity level is 3 when:

- Risk management is viewed as a business issue, and both the drawbacks and benefits of risk are recognized.
- There is a selected leader for risk management, engaged with the enterprise risk committee, across the enterprise.
- The business knows how IT fits in the enterprise risk universe and the risk portfolio view.
- Local tolerances drive the enterprise risk tolerance.
- Risk management activities are being aligned across the enterprise.

- Formal risk categories are identified and described in clear terms.
- Situations and scenarios are included in risk awareness training beyond specific policy and structures and promote a common language for communicating risk.
- Defined requirements exist for a centralized inventory of risk issues.
- Workflow tools are used to accelerate risk issues and track decisions.

Incorrect Answers:
C: Enterprise having risk management capability maturity level 5 requires continuous improvement of risk management skills, based on clearly defined personal and enterprise goals.

QUESTION 12
Which of the following role carriers is accounted for analyzing risks, maintaining risk profile, and risk-aware decisions?

A. Business management
B. Business process owner
C. Chief information officer (CIO)
D. Chief risk officer (CRO)

Answer: D
Explanation:
Business management is the business individuals with roles relating to managing a program. They are typically accountable for analyzing risks, maintaining risk profile, and risk-aware decisions. Other than this, they are also responsible for managing risks, react to events, etc.
Incorrect Answers:
B: Business process owner is an individual responsible for identifying process requirements, approving process design and managing process performance. He/she is responsible for analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.
C: CIO is the most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. CIO has some responsibility analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.

QUESTION 13
You are using Information system. You have chosen a poor password and also sometimes transmits data over unprotected communication lines. What is this poor quality of password and unsafe transmission refers to?

A. Probabilities
B. Threats
C. Vulnerabilities
D. Impacts

Answer: C
Explanation:
Vulnerabilities represent characteristics of information resources that may be exploited by a threat. The given scenario describes such a situation, hence it is a vulnerability.
Incorrect Answers:
A: Probabilities represent the likelihood of the occurrence of a threat, and this scenario does not describe a probability.
B: Threats are circumstances or events with the potential to cause harm to information resources. This scenario does not describe a threat.

D: Impacts represent the outcome or result of a threat exploiting a vulnerability. The stem does not describe an impact.

QUESTION 14

Which of the following is the BEST way to ensure that outsourced service providers comply with the enterprise's information security policy?

A. Penetration testing
B. Service level monitoring
C. Security awareness training
D. Periodic audits

Answer: D
Explanation:
As regular audits can spot gaps in information security compliance, periodic audits can ensure that outsourced service provider comply with the enterprise's information security policy.
Incorrect Answers:
A: Penetration testing can identify security vulnerability, but cannot ensure information compliance.
B: Service level monitoring can only identify operational issues in the enterprise's operational environment.
It does not play any role in ensuring that outsourced service provider complies with the enterprise's information security policy.
C: Training can increase user awareness of the information security policy, but is less effective than periodic auditing.

QUESTION 15

You are the project manager of RFT project. You have identified a risk that the enterprise's IT system and application landscape is so complex that, within a few years, extending capacity will become difficult and maintaining software will become very expensive. To overcome this risk, the response adopted is re- architecture of the existing system and purchase of new integrated system. In which of the following risk prioritization options would this case be categorized?

A. Deferrals
B. Quick win
C. Business case to be made
D. Contagious risk

Answer: C
Explanation:
This is categorized as a Business case to be made because the project cost is very large. The response to be implemented requires quite large investment. Therefore it comes under business case to be made.
Incorrect Answers:
A: It addresses costly risk response to a low risk. But here the response is less costly than that of business case to be made.
B: Quick win is very effective and efficient response that addresses medium to high risk. But in this the response does not require large investments.
D: This is not risk response prioritization option, instead it is a type of risk that happen with the several of the enterprise's business partners within a very short time frame.

QUESTION 16

Which of the following BEST ensures that a firewall is configured in compliance with an enterprise's security policy?

A. Interview the firewall administrator.
B. Review the actual procedures.
C. Review the device's log file for recent attacks.
D. Review the parameter settings.

Answer: D
Explanation:
A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide reliable audit evidence documentation.
Incorrect Answers:
A: While interviewing the firewall administrator may provide a good process overview, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.
B: While procedures may provide a good understanding of how the firewall is supposed to be managed, they do not reliably confirm that the firewall configuration complies with the enterprise's security policy.
C: While reviewing the device's log file for recent attacks may provide indirect evidence about the fact that logging is enabled, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

QUESTION 17
Which of following is NOT used for measurement of Critical Success Factors of the project?

A. Productivity
B. Quality
C. Quantity
D. Customer service

Answer: C
Explanation:
Incorrect Answers:
A, B, D: Productivity, quality and customer service are used for evaluating critical service factor of any particular project.

QUESTION 18
Which of the following statements is NOT true regarding the risk management plan?

A. The risk management plan is an output of the Plan Risk Management process.
B. The risk management plan is an input to all the remaining risk-planning processes.
C. The risk management plan includes a description of the risk responses and triggers.
D. The risk management plan includes thresholds, scoring and interpretation methods, responsible parties, and budgets.

Answer: C
Explanation:
The risk management plan details how risk management processes will be implemented, monitored, and controlled throughout the life of the project. The risk management plan does not include responses to risks or triggers. Responses to risks are documented in the risk register as part of the Plan Risk Responses process.
Incorrect Answers:

A, B, D: These all statements are true for risk management plan. The risk management plan details how risk management processes will be implemented, monitored, and controlled throughout the life of the project. It includes thresholds, scoring and interpretation methods, responsible parties, and budgets. It also act as input to all the remaining risk-planning processes.

QUESTION 19

You are the project manager of a project in Bluewell Inc. You and your project team have identified several project risks, completed risk analysis, and are planning to apply most appropriate risk responses. Which of the following tools would you use to choose the appropriate risk response?

A. Project network diagrams
B. Cause-and-effect analysis
C. Decision tree analysis
D. Delphi Technique

Answer: C

Explanation:

Decision tree analysis is a risk analysis tool that can help the project manager in determining the best risk response. The tool can be used to measure probability, impact, and risk exposure and how the selected risk response can affect the probability and/or impact of the selected risk event. It helps to form a balanced image of the risks and opportunities connected with each possible course of action. This makes them mostly useful for choosing between different strategies, projects, or investment opportunities particularly when the resources are limited. A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.

Incorrect Answers:

A: Project network diagrams help the project manager and stakeholders visualize the flow of the project work, but they are not used as a part of risk response planning.

B: Cause-and-effect analysis is used for exposing risk factors and not an effective one in risk response planning.

This analysis involves the use of predictive or diagnostic analytical tool for exploring the root causes or factors that contribute to positive or negative effects or outcomes.

D: Delphi technique is used for risk analysis, i.e., for identifying the most probable risks. Delphi is a group of experts who used to rate independently the business risk of an organization. Each expert analyzes the risk independently and then prioritizes the risk, and the result is combined into a consensus.

Thank You for Trying Our Product

Braindump2go Certification Features:

SATISFACTION 100% GUARANTEE

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

MONEY BACK 100% GUARANTEE

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

CISCO Microsoft CompTIA ORACLE

(ISC)² CiTRIX hp JUNIPer NETWORKS

CEH Certified Ethical Hacker EXIN EMC² where information lives

10% Discount Coupon Code: ASTR14