买题库
maitiku.com 专业题库供应商

Isaca

Exam CRISC

Certified in Risk and Information Systems Control

Version: 3.0

[Total Questions: 393]

http://www.maitiku.com QQ:860424807

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which of the following is the MOST important reason to maintain key risk indicators (KRIs)?

A. In order to avoid risk
B. Complex metrics require fine-tuning
C. Risk reports need to be timely
D. Threats and vulnerabilities change over time

Answer: D

Explanation:

Threats and vulnerabilities change over time and KRI maintenance ensures that KRIs continue to effectively capture these changes.

The risk environment is highly dynamic as the enterprise's internal and external environments are constantly changing. Therefore, the set of KRIs needs to be changed over time, so that they can capture the changes in threat and vulnerability.

Answer: B is incorrect. While most key risk indicator (KRI) metrics need to be optimized in respect to their sensitivity, the most important objective of KRI maintenance is to ensure that KRIs continue to effectively capture the changes in threats and vulnerabilities over time. Hence the most important reason is that because of change of threat and vulnerability overtime.

Answer: C is incorrect. Risk reporting timeliness is a business requirement, but is not a reason for KRI maintenance.

Answer: A is incorrect. Risk avoidance is one possible risk response. Risk responses are based on KRI reporting, but is not the reason for maintenance of KRIs.

Question No : 2 - (Topic 1)

You are the project manager of a HGT project that has recently finished the final compilation process. The project customer has signed off on the project completion and you have to do few administrative closure activities. In the project, there were several large risks that could have wrecked the project but you and your project team found some new methods to resolve the risks without affecting the project costs or project completion date. What should you do with the risk responses that you have identified during the project's

http://www.maitiku.com QQ:860424807

monitoring and controlling process?

A. Include the responses in the project management plan.
B. Include the risk responses in the risk management plan.
C. Include the risk responses in the organization's lessons learned database.
D. Nothing. The risk responses are included in the project's risk register already.

Answer: C

Explanation:

The risk responses that do not exist up till then, should be included in the organization's lessons learned database so other project managers can use these responses in their project if relevant.

Answer: D is incorrect. If the new responses that were identified is only included in the project's risk register then it may not be shared with project managers working on some other project.

Answer: A is incorrect. The responses are not in the project management plan, but in the risk response plan during the project and they'll be entered into the organization's lessons learned database.

Answer: B is incorrect. The risk responses are included in the risk response plan, but after completing the project, they should be entered into the organization's lessons learned database.

Question No : 3 - (Topic 1)

You are the project manager of GHT project. You have identified a risk event on your project that could save $100,000 in project costs if it occurs. Which of the following statements BEST describes this risk event?

A. This risk event should be mitigated to take advantage of the savings.
B. This is a risk event that should be accepted because the rewards outweigh the threat to the project.
C. This risk event should be avoided to take full advantage of the potential savings.
D. This risk event is an opportunity to the project and should be exploited.

Answer: D

Explanation:

This risk event has the potential to save money on project costs, so it is an opportunity, and the appropriate strategy to use in this case is the exploit strategy. The exploit response is

http://www.maitiku.com QQ:860424807

one of the strategies to negate risks or threats 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.

Answer: B is incorrect. To accept risk means that no action is taken relative to a particular risk; loss is accepted if it occurs. But as this risk event bring an opportunity, it should me exploited and not accepted.

Answer: A and C are incorrect. Mitigation and avoidance risk response is used in case of negative risk events, and not in positive risk events. Here in this scenario, as it is stated that the event could save $100,000, hence it is a positive risk event. Therefore should not be mitigated or avoided.

Question No : 4 - (Topic 1)

You are the project manager of a large construction project. This project will last for 18 months and will cost $750,000 to complete. You are working with your project team, experts, and stakeholders to identify risks within the project before the project work begins. Management wants to know why you have scheduled so many risk identification meetings throughout the project rather than just initially during the project planning. What is the best reason for the duplicate risk identification sessions?

A. The iterative meetings allow all stakeholders to participate in the risk identification processes throughout the project phases.
B. The iterative meetings allow the project manager to discuss the risk events which have passed the project and which did not happen.
C. The iterative meetings allow the project manager and the risk identification participants to identify newly discovered risk events throughout the project.
D. The iterative meetings allow the project manager to communicate pending risks events during project execution.

Answer: C

Explanation:

Risk identification is an iterative process because new risks may evolve or become known as the project progresses through its life cycle.

Answer: D is incorrect. The primary reason for iterations of risk identification is to identify new risk events.

Answer: B is incorrect. Risk identification focuses on discovering new risk events, not the

http://www.maitiku.com QQ:860424807

events which did not happen.
Answer: A is incorrect. Stakeholders are encouraged to participate in the risk identification process, but this is not the best choice for the

Question No : 5 - (Topic 1)

You are the risk official in Bluewell Inc. You are supposed to prioritize several risks. A risk has a rating for occurrence, severity, and detection as 4, 5, and 6, respectively. What Risk Priority Number (RPN) you would give to it?

A. 120
B. 100
C. 15
D. 30

Answer: A

Explanation:
Steps involving in calculating risk priority number are as follows:
Identify potential failure effects
Identify potential causes
Establish links between each identified potential cause
Identify potential failure modes
Assess severity, occurrence and detection
Perform score assessments by using a scale of 1 -10 (low to high rating) to score these assessments.
Compute the RPN for a particular failure mode as Severity multiplied by occurrence and detection.
RPN = Severity * Occurrence * Detection
Hence,
RPN = 4 * 5 * 6
= 120
Answer: C, D, and B are incorrect. These are not RPN for given values of severity, occurrence, and detection.

http://www.maitiku.com QQ:860424807

Question No : 6 - (Topic 1)

Which of the following is the MOST important use of KRIs?

A. Providing a backward-looking view on risk events that have occurred
B. Providing an early warning signal
C. Providing an indication of the enterprise's risk appetite and tolerance
D. Enabling the documentation and analysis of trends

Answer: B

Explanation:

Key Risk Indicators are the prime monitoring indicators of the enterprise. KRIs are highly relevant and possess a high probability of predicting or indicating important risk. KRIs help in avoiding excessively large number of risk indicators to manage and report that a large enterprise may have.

As KRIs are the indicators of risk, hence its most important function is to effectively give an early warning signal that a high risk is emerging to enable management to take proactive action before the risk actually becomes a loss.

Answer: D is incorrect. This is not as important as giving early warning.

Answer: A is incorrect. This is one of the important functions of KRIs which can help management to improve but is not as important as giving early warning.

Answer: C is incorrect. KRIs provide an indication of the enterprise's risk appetite and tolerance through metric setting, but this is not as important as giving early warning.

Question No : 7 - (Topic 1)

Which of the following role carriers will decide the Key Risk Indicator of the enterprise?

Each correct answer represents a part of the solution. Choose two.

A. Business leaders
B. Senior management
C. Human resource
D. Chief financial officer

Answer: A,B

Explanation:

An enterprise may have hundreds of risk indicators such as logs, alarms and reports. The

http://www.maitiku.com QQ:860424807

CRISC will usually need to work with senior management and business leaders to determine which risk indicators will be monitored on a regular basis and be recognized as KRIs.
Answer: D and C are incorrect. Chief financial officer and human resource only overview common risk view, but are not involved in risk based decisions.

Question No : 8 - (Topic 1)

What are the requirements for creating risk scenarios? Each correct answer represents a part of the solution. Choose three.

A. Determination of cause and effect
B. Determination of the value of business process at risk
C. Potential threats and vulnerabilities that could cause loss
D. Determination of the value of an asset

Answer: B,C,D

Explanation:
Creating a scenario requires determination of the value of an asset or a business process at risk and the potential threats and vulnerabilities that could cause loss. The risk scenario should be assessed for relevance and realism, and then entered into the risk register if found to be relevant.
In practice following steps are involved in risk scenario development:
First determine manageable set of scenarios, which include:
Frequently occurring scenarios in the industry or product area.
Scenarios representing threat sources that are increasing in count or severity level.
Scenarios involving legal and regulatory requirements applicable to the business.
After determining manageable risk scenarios, perform a validation against the business objectives of the entity.
Based on this validation, refine the selected scenarios and then detail them to a level in line with the criticality of the entity.
Lower down the number of scenarios to a manageable set. Manageable does not signify a fixed number, but should be in line with the overall importance and criticality of the unit.
Risk factors kept in a register so that they can be reevaluated in the next iteration and included for detailed analysis if they have become relevant at that time.
Risk factors kept in a register so that they can be reevaluated in the next iteration and included for detailed analysis if they have become relevant at that time.

http://www.maitiku.com QQ:860424807

Include an unspecified event in the scenarios, that is, address an incident not covered by other scenarios.
Answer: A is incorrect. Cause-and-effect analysis is a predictive or diagnostic analytical tool used to explore the root causes or factors that contribute to positive or negative effects or outcomes. It is used during the process of exposing risk factors.

Question No : 9 - (Topic 1)

You work as the project manager for Bluewell Inc. Your project has several risks that will affect several stakeholder requirements. Which project management plan will define who will be available to share information on the project risks?

A. Resource Management Plan
B. Risk Management Plan
C. Stakeholder management strategy
D. Communications Management Plan

Answer: D

Explanation:
The Communications Management Plan defines, in regard to risk management, who will be available to share information on risks and responses throughout the project.
The Communications Management Plan aims to define the communication necessities for the project and how the information will be circulated. The Communications Management Plan sets the communication structure for the project. This structure provides guidance forcommunication throughout the project's life and is updated as communication needs change. The Communication Managements Plan identifies and defines the roles of persons concerned with the project. It includes a matrix known as the communication matrix to map the communication requirements of the project.
Answer: C is incorrect. The stakeholder management strategy does not address risk communications.
Answer: B is incorrect. The Risk Management Plan defines risk identification, analysis, response, and monitoring.
Answer: A is incorrect. The Resource Management Plan does not define risk communications.

http://www.maitiku.com QQ:860424807

Question No : 10 - (Topic 1)

Which of the following controls is an example of non-technical controls?

A. Access control
B. Physical security
C. Intrusion detection system
D. Encryption

Answer: B

Explanation:

Physical security is an example of non-technical control. It comes under the family of operational controls.

Answer: C, A, and D are incorrect. Intrusion detection system, access control, and encryption are the safeguards that are incorporated into computer hardware, software or firmware, hence they refer to as technical controls.

Question No : 11 - (Topic 1)

You are the project manager of GHT project. Your project team is in the process of identifying project risks on your current project. The team has the option to use all of the following tools and techniques to diagram some of these potential risks EXCEPT for which one?

A. Process flowchart
B. Ishikawa diagram
C. Influence diagram
D. Decision tree diagram

Answer: D

Explanation:

Decision tree diagrams are used during the Quantitative risk analysis process and not in risk identification.

Answer: B, A, and C are incorrect.

All the these options are diagrammatical techniques used in the Identify risks process.

http://www.maitiku.com QQ:860424807

Question No : 12 - (Topic 1)

Which of the following BEST describes the utility of a risk?

A. The finance incentive behind the risk
B. The potential opportunity of the risk
C. The mechanics of how a risk works
D. The usefulness of the risk to individuals or groups

Answer: D

Explanation:

The utility of the risk describes the usefulness of a particular risk to an individual. Moreover, the same risk can be utilized by two individuals in different ways. Financial outcomes are one of the methods for measuring potential value for taking a risk. For example, if the individual's economic wealth increases, the potential utility of the risk will decrease.

Answer: C is incorrect. It is not the valid definition.

Answer: A is incorrect. Determining financial incentive is one of the method to measure the potential value for taking a risk, but it is not the valid definition for utility of risk.

Answer: B is incorrect. It is not the valid definition.

Question No : 13 - (Topic 1)

Which of the following aspect of monitoring tool ensures that the monitoring tool has the ability to keep up with the growth of an enterprise?

A. Scalability
B. Customizability
C. Sustainability
D. Impact on performance

Answer: A

Explanation:

Monitoring tools have to be able to keep up with the growth of an enterprise and meet anticipated growth in process, complexity or transaction volumes; this is ensured by the scalability criteria of the monitoring tool.

Answer: C is incorrect. It ensures that monitoring software is able to change at the same speed as technology applications and infrastructure to be effective over time.

Answer: B is incorrect. For software to be effective, it must be customizable to the specific

http://www.maitiku.com QQ:860424807