ISACA

CRISC

Certified in Risk and Information Systems Control

http://killexams.com/pass4sure/exam-detail/CRISC
Question: 521
Which of the following components of risk scenarios has the potential to generate internal or external threat on an enterprise?
A. Timing dimension
B. Events
C. Assets
D. Actors

Answer: D

Explanation:
Components of risk scenario that are needed for its analysis are:
Actor: Actors are those components of risk scenario that has the potential to generate the threat that can be internal or external, human or non-human. Internal actors are within the enterprise like staff, contractors, etc. On the other hand, external actors include outsiders, competitors, regulators and the market.
Threat type: Threat type defines the nature of threat, that is, whether the threat is malicious, accidental, natural or intentional.
Event: Event is an essential part of a scenario; a scenario always has to contain an event. Event describes the happenings like whether it is a disclosure of confidential information, or interruption of a system or project, or modification, theft, destruction, etc. Asset: Assets are the economic resources owned by business or company. Anything tangible or intangible that one possesses, usually considered as applicable to the payment of one’s debts, is considered an asset. An asset can also be defined as a resource, process, product, computing infrastructure, and so forth that an organization has determined must be protected. Tangible asset: Tangible are those asset that has physical attributes and can be detected with the senses, e.g., people, infrastructure, and finances. Intangible asset: Intangible are those asset that has no physical attributes and cannot be detected with the senses, e.g., information, reputation and customer trust.
Timing dimension: The timing dimension is the application of the scenario to detect time to respond to or recover from an event. It identifies if the event occur at a critical moment and its duration. It also specifies the time lag between the event and the consequence, that is, if there an immediate consequence (e.g., network failure, immediate downtime) or a delayed consequence (e.g., wrong IT architecture with accumulated high costs over a long period of time).

Question: 522
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 needs of an enterprise. Hence customizability ensures that end users can adapt the software. Answer: D is incorrect. The impact on performance has nothing related to the ability of monitoring tool to keep up with the growth of enterprise.

Question: 523
You are the project manager in your enterprise. You have identified risk that is noticeable failure threatening the success of certain goals of your enterprise. In which of the following levels do this identified risk exists?
A. Moderate risk
B. High risk
C. Extremely high risk
D. Low risk

Answer: A
Explanation:
Moderate risks are noticeable failure threatening the success of certain goals. Answer: C is incorrect. Extremely high risk are the risks that has large impact on enterprise and are most likely results in failure with severe consequences. Answer: B is incorrect. High risk is the significant failure impacting in certain goals not being met.
Answer: D is incorrect. Low risks are the risk that results in certain unsuccessful goals.

Question: 524
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 for communication 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.

Question: 525
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: 526
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.

Question: 527
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
Question: 528

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: 529

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 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: 530

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: DBC

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. 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.
For More exams visit https://killexams.com/vendors-exam-list

Kill your exam at First Attempt....Guaranteed!