ISACA CRISC (*Certified in Risk and Information Systems Control)*

Question: 1

Assessing the probability and consequences of identified risks to the project objectives, assigning a risk score to each risk, and creating a list of prioritized risks describes which of the following processes?

A. Identify Risks

B. Qualitative Risk Analysis

C. Quantitative Risk Analysis

D. Plan Risk Management

Answer: B

Explanation:

The purpose of qualitative risk analysis is to determine what impact the identified risk events will have on the project and the probability they'll occur. It also puts risks in priority order according to their effects on the project objectives and assigns a risk score for the project.

Answer: C is incorrect. This process does not involve assessing the probability and consequences of identified risks. Quantitative analysis is the use of numerical and statistical techniques rather than the analysis of verbal material for analyzing risks. Some of the quantitative methods of risk analysis are:

Internal loss method

External data analysis

Business process modeling (BPM) and simulation

Statistical process control (SPC)

Answer: A is incorrect. It involves listing of all the possible risks so as to cure them before it can occur. In risk identification both threats and opportunities are considered, as both carry some level of risk with them.

Answer: D is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Assessing the probability and consequences of identified risks is only the part of risk management.

Question: 2

Which of the following characteristics of baseline represents specification that is used to identify approved requirements in baseline modeling?

A. Functional
B. Allocated
C. Product
D. Developmental

Answer: B

Explanation:
In baseline modeling, the baseline can characterize the functional, allocated, developmental, and product aspects of a solution. The allocated characteristic focus on the specifications which met the requirements approved by management.

Answer: A, C, and D are incorrect. These characteristics do not represents specification that is used to identify approved requirements in baseline modeling.

Question: 3

Which of the following variables are associated with quantitative assessment of risks?
Each correct answer represents a complete solution. Choose three.

A. Impact
B. Probability
C. Cost
D. Frequency

Answer: D, B, and A

Explanation:
The measurable data used by this assessment include frequency, probability, impact, and effectiveness of countermeasures.
Risk assessment is a process of analyzing the identified risk, both quantitatively and qualitatively.
Quantitative risk assessment requires calculations of two components of risk, the magnitude of the potential loss, and the probability that the loss will occur. While qualitatively risk assessment checks the severity of risk. The assessment attempts to determine the likelihood of the risk being realized and the impact of the risk on the operation. This provides several conclusions:
Probability-establishing the likelihood of occurrence and reoccurrence of specific risks, independently and combined.
Interdependencies-the relationship between different types of risk. For instance, one risk may have greater potential of occurring if another risk has occurred. Or probability or impact of a situation may increase with combined risk.

Question: 4

Which of the following laws applies to organizations handling health care information?
A. SOX
B. GLBA
C. HIPAA
D. FISMA

Answer: C

Explanation:
HIPAA handles health care information of an organization.
The Health Insurance Portability and Accountability Act (HIPAA) were introduced in 1996. It ensures that health information data is protected. Before HIPAA, personal medical information was often available to anyone. Security to protect the data was lax, and the data was often misused.
If your organization handles health information, HIPAA applies. HIPAA defines health information as any data that is created or received by health care providers, health plans, public health authorities, employers, life insurers, schools or universities, and health care clearinghouses.
HIPAA defines any data that is related to the health of an individual, including past/present/future health, physical/mental health, and past/present/future payments for health care.
Creating a HIPAA compliance plan involves following phases:
Assessment: An assessment helps in identifying whether organization is covered by HIPAA. If it is, then further requirement is to identify what data is needed to protect.
Risk analysis: A risk analysis helps to identify the risks. In this phase, analyzing method of handling data of organization is done.
Plan creation: After identifying the risks, plan is created. This plan includes methods to reduce the risk.
Plan implementation: In this plan is being implemented.
Continuous monitoring: Security in depth requires continuous monitoring. Monitor regulations for changes. Monitor risks for changes.
Monitor the plan to ensure it is still used.
Assessment: Regular reviews are conducted to ensure that the organization remains in compliance.

Answer: A is incorrect. SOX designed to hold executives and board members personally responsible for financial data.

Answer: B is incorrect. GLBA is not used for handling health care information.

Answer: D is incorrect. FISMA ensures protection of data of federal agencies.

Question: 5

You are the project manager of GRT project. You discovered that by bringing on more qualified resources or by providing even better quality than originally planned, could result in reducing the amount of time required to complete the project. If your organization seizes this opportunity it would be an example of what risk response?

A. Share
B. Enhance
C. Exploit
D. Accept

Answer: C

Explanation:
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.

Answer: A is incorrect. - The share strategy is similar as transfer because in this a portion of the risk is shared with an external organization or another internal entity.

Answer: B is incorrect. The enhance strategy closely watches the probability or impact of the risk event to assure that the organization realizes the benefits. The primary point of this strategy is to attempt to increase the probability and/or impact of positive risks.

Answer: D is incorrect. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs.

Question: 6

You are the project manager of the NHQ project in Bluewell Inc. The project has an asset valued at $200,000 and is subjected to an exposure factor of 45 percent. If the annual rate of occurrence of loss in this project is once a month, then what will be the Annual Loss Expectancy (ALE) of the project?

A. $ 2,160,000
B. $ 95,000
C. $ 90,000
D. $ 108,000

Answer: D

Explanation:
The ALE of this project will be $ 108,000.
Single Loss Expectancy is a term related to Quantitative Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows:

SLE = Asset value * Exposure factor
Therefore,
SLE = 200,000 * 0.45
= $ 90,000
As the loss is occurring once every month, therefore ARO is 12. Now ALE can be calculated as follows:
ALE = SLE * ARO
= 90,000 * 12
= $ 108,000

Question: 7

Which of the following is NOT true for Key Risk Indicators?
A. The complete set of KRIs should also balance indicators for risk, root causes and business impact.
B. They help avoid having to manage and report on an excessively large number of risk indicators
C. They are monitored annually
D. They are selected as the prime monitoring indicators for the enterprise

Answer: C

Explanation:
They are monitored on regular basis as they indicate high probability and high impact risks. As risks change over time, hence KRIs should also be monitored regularly for its effectiveness on these changing risks.

Answer: D, B, and A are incorrect. These all are true for KRIs. 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.
The complete set of KRIs should also balance indicators for risk, root causes and business impact, so as to indicate the risk and its impact completely.

Question: 8

You work as a project manager for SoftTech Inc. You are working with the project stakeholders to begin the qualitative risk analysis process.
Which of the following inputs will be needed for the qualitative risk analysis process in your project?
Each correct answer represents a complete solution. Choose all that apply.
A. Cost management plan
B. Organizational process assets
C. Project scope statement
D. Risk register

Answer: D, B, and C

Explanation:
The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are:
Organizational process assets
Project Scope Statement
Risk Management Plan
Risk Register

Answer: A is incorrect. The cost management plan is the input to perform quantitative risk analysis process.

Question: 9

You have identified several risks in your project. You have opted for risk mitigation in order to respond to identified risk. Which of the following ensures that risk mitigation method that you have chosen is effective?
A. Reduction in the frequency of a threat
B. Minimization of inherent risk
C. Reduction in the impact of a threat
D. Minimization of residual risk

Answer: B

Explanation:
The inherent risk of a process is a given and cannot be affected by risk reduction or risk mitigation efforts. Hence it should be reduced as far as possible.

Answer: D is incorrect. The objective of risk reduction is to reduce the residual risk to levels below the enterprise's risk tolerance level.

Answer: A is incorrect. Risk reduction efforts can focus on either avoiding the frequency of the risk or reducing the impact of a risk.

Answer: C is incorrect. Risk reduction efforts can focus on either avoiding the frequency of the risk or reducing the impact of a risk.

Question: 10

Which of the following methods involves the use of predictive or diagnostic analytical tool for exposing risk factors?
A. Fault tree analysis
B. Scenario analysis
C. Sensitivity analysis
D. Cause and effect analysis

Answer: D