Braindumps.CRISC.393.QA

Number: CRISC
Passing Score: 800
Time Limit: 120 min
File Version: 37.1

VCEplus.com

CRISC

CERTIFIED IN RISK AND INFORMATION SYSTEMS CONTROL

- Corrected many of questions answers after confirmation.
- This exam tools have really helped me to gain a command on the entire course.
- Passed!!!!!! I did it! The credit of my success however actually goes to this brain dump study material that sharpened my knowledge and provided me practical exposure through practice test Questions.
- I only used these questions and got 900 marks with this. Perfect Show.
- There is a high probability you will pass your exam with highest score.
- Here the secret to pass certification exam in first attempt.

BrainDumps

Sections

1. Volume A
2. Volume B
3. Volume C
4. Volume D

Exam A

QUESTION 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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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 2
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.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

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 3
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

Correct Answer: DBC
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 4
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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 5
Which of the following controls is an example of non-technical controls?

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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
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 6
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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 7
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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 8
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
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 9
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
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 10

Courtney is the project manager for her organization. She is working with the project team to complete the qualitative risk analysis for her project. During the analysis Courtney encourages the project team to begin the grouping of identified risks by common causes. What is the primary advantage to group risks by common causes during qualitative risk analysis?

A. It helps the project team realize the areas of the project most laden with risks.
B. It assist in developing effective risk responses.
C. It saves time by collecting the related resources, such as project team members, to analyze the risk events.
D. It can lead to the creation of risk categories unique to each project.

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
By grouping the risks by categories the project team can develop effective risk responses. Related risk events often have common causal factors that can be addressed with a single risk response.

QUESTION 11
Which of the following processes is described in the statement below? "It is the process of exchanging information and views about risks among stakeholders, such as groups, individuals, and institutions."

A. Risk governance
B. Risk identification
C. Risk response planning
D. Risk communication

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Risk communication is the process of exchanging information and views about risks among stakeholders, such as groups, individuals, and institutions. Risk communication is mostly concerned with the nature of risk or expressing concerns, views, or reactions to risk managers or institutional bodies for risk management. The key plan to consider and communicate risk is to categorize and impose priorities, and acquire suitable measures to reduce risks. It is important throughout any crisis to put across multifaceted information in a simple and clear manner.
Risk communication helps in switching or allocating the information concerning risk among the decision-maker and the stakeholders. Risk communication can be explained more clearly with the help of the following definitions:
It defines the issue of what a group does, not just what it says. It must take into account the valuable element in user's perceptions of risk. It will be more valuable if

it is thought of as conversation, not instruction. Risk communication is a fundamental and continuing element of the risk analysis exercise, and the involvement of the stakeholder group is from the beginning. It makes the stakeholders conscious of the process at each phase of the risk assessment. It helps to guarantee that the restrictions, outcomes, consequence, logic, and risk assessment are undoubtedly understood by all the stakeholders.
Answer: C is incorrect. A risk response ensures that the residual risk is within the limits of the risk appetite and tolerance of the enterprise. Risk response is process of selecting the correct, prioritized response to risk, based on the level of risk, the enterprise's risk tolerance and the cost and benefit of the particular risk response option. Risk response ensures that management is providing accurate reports on:
The level of risk faced by the enterprise
The incidents' type that have occurred
Any alteration in the enterprise's risk profile based on changes in the risk environment

QUESTION 12
You are an experienced Project Manager that has been entrusted with a project to develop a machine which produces auto components. You have scheduled meetings with the project team and the key stakeholders to identify the risks for your project. Which of the following is a key output of this process?

A. Risk Register
B. Risk Management Plan
C. Risk Breakdown Structure
D. Risk Categories

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The primary outputs from Identify Risks are the initial entries into the risk register. The risk register ultimately contains the outcomes of other risk management processes as they are conducted, resulting in an increase in the level and type of information contained in the risk register over time.
Answer: B, D, and C are incorrect. All these are outputs from the "Plan Risk Management" process, which happens prior to the starting of risk identification.

QUESTION 13
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:

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 14

You are the project manager of GHT project. You have planned the risk response process and now you are about to implement various controls. What you should do before relying on any of the controls?

A. Review performance data

B. Discover risk exposure

C. Conduct pilot testing

D. Articulate risk

Correct Answer: AC

Section: Volume A

Explanation

Explanation/Reference:

Explanation:

Pilot testing and reviewing of performance data to verify operation against design are done before relying on control.

Answer: D is incorrect. Articulating risk is the first phase in the risk response process to ensure that information on the true state of exposures and opportunities are made available in a timely manner and to the right people for appropriate response. But it does not play any role in identifying whether any specific control is reliable or not. Answer: B is incorrect. Discovering risk exposure helps in identifying the severity of risk, but it does not play any role in specifying the reliability of control.

QUESTION 15

Which of the following is NOT true for risk management capability maturity level 1?

A. There is an understanding that risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk
B. Decisions involving risk lack credible information
C. Risk appetite and tolerance are applied only during episodic risk assessments
D. Risk management skills exist on an ad hoc basis, but are not actively developed

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The enterprise with risk management capability maturity level 0 makes decisions without having much knowledge about the risk credible information. In level 1, enterprise takes decisions on the basis of risk credible information.
Answer: A, C, and D are incorrect.
An enterprise's risk management capability maturity level is 1 when:
There is an understanding that risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk. Any risk identification criteria vary widely across the enterprise. Risk appetite and tolerance are applied only during episodic risk assessments. Enterprise risk policies and standards are incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms. Risk management skills exist on an ad hoc basis, but are not actively developed. Ad hoc inventories of controls that are unrelated to risk are dispersed across desktop applications.

QUESTION 16
Which of the following is true for Cost Performance Index (CPI)?

A. If the CPI > 1, it indicates better than expected performance of project
B. CPI = Earned Value (EV) * Actual Cost (AC)
C. It is used to measure performance of schedule
D. If the CPI = 1, it indicates poor performance of project

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Cost performance index (CPI) is used to calculate performance efficiencies of project. It is used in trend analysis to predict future performance. CPI is the ratio of earned value to actual cost.
If the CPI value is greater than 1, it indicates better than expected performance, whereas if the value is less than 1, it shows poor performance.
Answer: C is incorrect. Cost performance index (CPI) is used to calculate performance efficiencies of project and not its schedule.
Answer: B is incorrect. CPI is the ratio of earned value to actual cost, i.e., CPI = Earned Value (EV) / Actual Cost (AC).

Answer: D is incorrect. The CPI value of 1 indicates that the project is right on target.

QUESTION 17
Which of the following do NOT indirect information?

A. Information about the propriety of cutoff
B. Reports that show orders that were rejected for credit limitations.
C. Reports that provide information about any unusual deviations and individual product margins.
D. The lack of any significant differences between perpetual levels and actual levels of goods.

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Information about the propriety of cutoff is a kind of direct information. Answer: C is incorrect. Reports that provide information about any unusual deviations and individual product margins (whereby, the price of an item sold is compared to its standard cost) provide indirect information that controls over billing and pricing are operating. Answer: B is incorrect. Reports that show orders that were rejected for credit limitations provide indirect information that credit checking aspects of the system are working as intended.
Answer: D is incorrect. The lack of any significant differences between perpetual levels and actual levels provides indirect information that its billing controls are operating.

QUESTION 18
Ben works as a project manager for the MJH Project. In this project, Ben is preparing to identify stakeholders so he can communicate project requirements, status, and risks. Ben has elected to use a salience model as part of his stakeholder identification process. Which of the following activities best describes a salience model?

A. Describing classes of stakeholders based on their power (ability to impose their will), urgency (need for immediate attention), and legitimacy (their involvement is appropriate).
B. Grouping the stakeholders based on their level of authority ("power") and their level or concern ("interest") regarding the project outcomes.
C. Influence/impact grid, grouping the stakeholders based on their active involvement ("influence") in the project and their ability to affect changes to the project's planning or execution ("impact").
D. Grouping the stakeholders based on their level of authority ("power") and their active involvement ("influence") in the project.

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

Explanation:
A salience model defines and charts stakeholders' power, urgency, and legitimacy in the project.
The salience model is a technique for categorizing stakeholders according to their importance. The various difficulties faced by the project managers are as follows:
How to choose the right stakeholders?
How to prioritize competing claims of the stakeholders communication needs? Stakeholder salience is determined by the evaluation of their power, legitimacy and urgency in the organization.
Power is defined as the ability of the stakeholder to impose their will.
Urgency is the need for immediate action.
Legitimacy shows the stakeholders participation is appropriate or not. . The model allows the project manager to decide the relative salience of a particular stakeholder.
Answer: B is incorrect. This defines the power/interest grid. Answer: D is incorrect. This defines a power/influence grid. Answer: C is incorrect. This defines an influence/impact grid.

QUESTION 19
Which of the following is the first MOST step in the risk assessment process?

A. Identification of assets
B. Identification of threats
C. Identification of threat sources
D. Identification of vulnerabilities

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Asset identification is the most crucial and first step in the risk assessment process. Risk identification, assessment and evaluation (analysis) should always be clearly aligned to assets. Assets can be people, processes, infrastructure, information or applications.

QUESTION 20
Which of the following matrices is used to specify risk thresholds?

A. Risk indicator matrix
B. Impact matrix
C. Risk scenario matrix
D. Probability matrix

Correct Answer: A

Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Risk indicators are metrics used to indicate risk thresholds, i.e., it gives indication when a risk level is approaching a high or unacceptable level of risk. The main objective of a risk indicator is to ensure tracking and reporting mechanisms that alert staff about the potential risks.
Answer: D and B are incorrect. Estimation of risk's consequence and priority for awareness is conducted by using probability and impact matrix. These matrices specify the mixture of probability and impact that directs to rating the risks as low, moderate, or high priority. Answer: C is incorrect. A risk scenario is a description of an event that can lay an impact on business, when and if it would occur.
Some examples of risk scenario are of:
Having a major hardware failure
Failed disaster recovery planning (DRP)
Major software failure

QUESTION 21
What are the two MAJOR factors to be considered while deciding risk appetite level? Each correct answer represents a part of the solution. Choose two.

A. The amount of loss the enterprise wants to accept
B. Alignment with risk-culture
C. Risk-aware decisions
D. The capacity of the enterprise's objective to absorb loss.

Correct Answer: AD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
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. Answer: B is incorrect. Alignment with risk-culture is also one of the factors but is not as important as these two.
Answer: C is incorrect. Risk aware decision is not the factor, but is the result which uses risk appetite information as its input.

QUESTION 22
You are the project manager of the GHY Project for your company. You need to complete a project management process that will be on the lookout for new risks, changing risks, and risks that are now outdated. Which project management process is responsible for these actions?

A. Risk planning

B. Risk monitoring and controlling

C. Risk identification

D. Risk analysis

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The risk monitoring and controlling is responsible for identifying new risks, determining the status of risks that may have changed, and determining which risks may be outdated in the project.
Answer: C is incorrect. Risk identification is a process that identifies risk events in the project.
Answer: A is incorrect. Risk planning creates the risk management plan and determines how risks will be identified, analyzed, monitored and controlled, and responded to. Answer: D is incorrect. Risk analysis helps determine the severity of the risk events, the risks' priority, and the probability and impact of risks.

QUESTION 23
You are the project manager of the HGT project in Bluewell Inc. The project has an asset valued at $125,000 and is subjected to an exposure factor of 25 percent. What will be the Single Loss Expectancy of this project?

A. $ 125,025

B. $ 31,250

C. $ 5,000

D. $ 3,125,000

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The Single Loss Expectancy (SLE) of this project will be $31,250. 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:
Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor represents the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two third, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed.
Therefore,
SLE = Asset Value * Exposure Factor
= 125,000 * 0.25
= $31,250

Answer: D, C, and A are incorrect.
These are not SLEs of this project.

QUESTION 24
Where are all risks and risk responses documented as the project progresses?

A. Risk management plan
B. Project management plan
C. Risk response plan
D. Risk register

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
All risks, their responses, and other characteristics are documented in the risk register. As the project progresses and the conditions of the risk events change, the risk register should be updated to reflect the risk conditions.
Answer: A is incorrect. The risk management plan addresses the project management's approach to risk management, risk identification, analysis, response, and control. Answer: C is incorrect. The risk response plan only addresses the planned risk responses for the identified risk events in the risk register.
Answer: B is incorrect. The project management plan is the overarching plan for the project, not the specifics of the risk responses and risk identification.

QUESTION 25
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

A. Transference
B. Mitigation
C. Avoidance
D. Exploit

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
When you are hiring a third party to own risk, it is known as transference risk response. Risk transfer means that impact of risk is reduced by transferring or otherwise sharing a portion of the risk with an external organization or another internal entity. Transfer of risk can occur in many forms but is most effective when

dealing with financial risks. Insurance is one form
of risk transfer.
Answer: B is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation.
Answer: D is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Answer: C is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

QUESTION 26
John works as a project manager for BlueWell Inc. He is determining which risks can affect the project. Which of the following inputs of the identify risks process is useful in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk?

A. Activity duration estimates
B. Activity cost estimates
C. Risk management plan
D. Schedule management plan

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The activity duration estimates review is valuable in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk.
Answer: B is incorrect. The activity cost estimates review is valuable in identifying risks as it provides a quantitative assessment of the expected cost to complete scheduled activities and is expressed as a range, with a width of the range indicating the degrees of risk. Answer: D is incorrect. It describes how the schedule contingencies will be reported and assessed.
Answer: C is incorrect. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix.

QUESTION 27
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

Correct Answer: BCD
Section: Volume A
Explanation

Explanation/Reference:
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
Answer: A is incorrect. Someone sees company's secret formula or password comes under loss of confidentiality.

QUESTION 28
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
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.
Answer: B is incorrect. Review of the existing IT environment is also useful and necessary but is not the first step that needs to be undertaken. Answer: D is incorrect. The present IT budget is just one of the components of the strategic plan.
Answer: A is incorrect. The IT strategic plan exists to support the enterprise's strategic plan but is not solely considered while designing information system control.

QUESTION 29
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

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. Answer: A is incorrect. This is the consequence of poor risk communication, not the inhibitor of effective communication.
Answer: D is incorrect. 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.
Answer: B is incorrect. . This is the consequence of poor risk communication, not the inhibitor of effective communication.

QUESTION 30
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.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Low-impact, low-probability risks can be added to the low priority risk watch list. Answer: B is incorrect. 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.
Answer: A is incorrect. These risks are not dismissed; they are still documented on the low priority risk watch list.
Answer: D is incorrect. Not every risk demands a risk response, so this choice is incorrect.

QUESTION 31
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

Correct Answer: A

Section: Volume A
Explanation

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

QUESTION 32
What are the functions of audit and accountability control? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ACD
Section: Volume A
Explanation

Explanation/Reference:
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.
Answer: B is incorrect. 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 33
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
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.
Answer: C and A are incorrect. 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 followingtwo 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. Answer: D is incorrect. 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 34
What is the value of exposure factor if the asset is lost completely?

A. 1

B. Infinity

C. 10

D. 0

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
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. Answer: B, D, and C are incorrect. These are not the values of exposure factor for zero assets.

QUESTION 35
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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. Answer: C is incorrect. Opportunistic is not a valid risk response. Answer: B is incorrect. This is an example of a positive risk, but positive is not a risk response.
Answer: A is incorrect. Enhancing is a positive risk response that describes actions taken to increase the odds of a risk event to happen.

QUESTION 36
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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. Answer: C, A, and B are incorrect. These are wrong formulas and are not used in quantitative risk assessment.

QUESTION 37
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

Correct Answer: ABD
Section: Volume A
Explanation

Explanation/Reference:
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. Answer: C is incorrect. Enterprise having risk management capability maturity level 5 requires continuous improvement of risk management skills, based on clearly defined personal and enterprise goals.

QUESTION 38
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)

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
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. Answer: C is incorrect. 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.
Answer: B is incorrect. 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.
Answer: D is incorrect. CRO is the individual who oversees all aspects of risk management across the enterprise. He/she is responsible for analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.

QUESTION 39
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
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. Answer: B is incorrect. Threats are circumstances or events with the potential to cause harm to information resources. This scenario does not describe a threat. Answer: A is incorrect. Probabilities represent the likelihood of the occurrence of a threat, and this scenario does not describe a probability.
Answer: D is incorrect. Impacts represent the outcome or result of a threat exploiting a vulnerability. The stem does not describe an impact.

QUESTION 40
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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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.
Answer: C is incorrect. Training can increase user awareness of the information security policy, but is less effective than periodic auditing. Answer: A is incorrect. Penetration testing can identify security vulnerability, but cannot ensure information compliance.
Answer: B is incorrect. 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 comply with the enterprise's information security policy.

QUESTION 41
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
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.
Answer: B is incorrect. Quick win is very effective and efficient response that addresses medium to high risk. But in this the response does not require large investments. Answer: A is incorrect. It addresses costly risk response to a low risk. But here the response is less costly than that of business case to be made.
Answer: D is incorrect. 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 42
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.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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. Answer: B is incorrect. 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. Answer: A is incorrect. 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.
Answer: C is incorrect. 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 43
Which of following is NOT used for measurement of Critical Success Factors of the project?

A. Productivity

B. Quality

C. Quantity

D. Customer service

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Answer: A, B, and D are incorrect. Productivity, quality and customer service are used for evaluating critical service factor of any particular project.

QUESTION 44
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.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
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. Answer: A, D, and B are incorrect. 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 45
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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
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 oppourtunities 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. Answer: D is incorrect. 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.
Answer: A is incorrect. 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.
Answer: B is incorrect. 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.

QUESTION 46
You are the risk official of your enterprise. Your enterprise takes important decisions without considering risk credential information and is also unaware of external requirements for risk management and integration with enterprise risk management. In which of the following risk management capability maturity levels does your enterprise exists?

A. Level 1
B. Level 0
C. Level 5
D. Level 4

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
0 nonexistent: An enterprise's risk management capability maturity level is 0 when:
The enterprise does not recognize the need to consider the risk management or the business impact from IT risk.
Decisions involving risk lack credible information. Awareness of external requirements for risk management and integration with enterprise risk management (ERM) do not exists.
Answer: A, C, and D are incorrect.
These all are much higher levels of the risk management capability maturity model and in all these enterprise do take decisions considering the risk credential information. Moreover, in these levels enterprise is aware of external requirements for risk management and integrate with ERM.

QUESTION 47
Which of the following is the priority of data owners when establishing risk mitigation method?

A. User entitlement changes
B. Platform security
C. Intrusion detection
D. Antivirus controls

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

Explanation:
Data owners are responsible for assigning user entitlement changes and approving access to the systems for which they are responsible.
Answer: C, B, and D are incorrect. Data owners are not responsible for intrusion detection, platform security or antivirus controls.
These are the responsibilities of data custodians.

QUESTION 48
What type of policy would an organization use to forbid its employees from using organizational e-mail for personal use?

A. Anti-harassment policy
B. Acceptable use policy
C. Intellectual property policy
D. Privacy policy

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
An acceptable use policy is a set of rules applied by the owner/manager of a network, website or large computer system that restrict the ways in which the network site or system may be used. Acceptable Use Policies are an integral part of the framework of information security policies.
Answer: D is incorrect. Privacy policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data.
Answer: C and A are incorrect. These two policies are not related to Information system security.

QUESTION 49
Wendy has identified a risk event in her project that has an impact of $75,000 and a 60 percent chance of happening. Through research, her project team learns that the risk impact can actually be reduced to just $15,000 with only a ten percent chance of occurring. The proposed solution will cost $25,000. Wendy agrees to the $25,000 solution. What type of risk response is this?

A. Mitigation
B. Avoidance
C. Transference
D. Enhancing

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:

Explanation:
Risk mitigation implies a reduction in the probability and/or impact of an adverse risk event to be within acceptable threshold limits. Taking early actions to reduce the probability and/or impact of a risk occurring on the project is often more effective than trying to repair the damage after the risk has occurred.
Answer: B is incorrect. Avoidance changes the project plan to avoid the risk altogether. Answer: C is incorrect. Transference requires shifting some or all of the negative impacts of a threat, along with the ownership of the response, to a third party. Transferring the risk simply gives another party the responsibility for its management-it does not eliminate it. Transferring the liability for a risk is most effective in dealing with financial risk exposure. Risk transference nearly always involves payment of a risk premium to the party taking on the risk.
Answer: D is incorrect. Enhancing is actually a positive risk response. This strategy is used to increase the probability and/or the positive impact of an opportunity. Identifying and maximizing the key drivers of these positive-impact risks may increase the probability of their occurrence.

QUESTION 50
Which of the following processes addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget?

A. Monitor and Control Risk
B. Plan risk response
C. Identify Risks
D. Qualitative Risk Analysis

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The plan risk response project management process aims to reduce the threats to the project objectives and to increase opportunities. It follows the perform qualitative risk analysis process and perform quantitative risk analysis process. Plan risk response process includes the risk response owner to take the job for each agreed-to and funded risk response. This process addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget. The inputs to the plan risk response process are as follows:
Risk register
Risk management plan
Answer: C is incorrect. Identify Risks is the process of determining which risks may affect the project. It also documents risks' characteristics. The Identify Risks process is part of the Project Risk Management knowledge area. As new risks may evolve or become known as the project progresses through its life cycle, Identify Risks is an iterative process. The process should involve the project team so that they can develop and maintain a sense of ownership and responsibility for the risks and associated risk response actions. Risk Register is the only output of this process.
Answer: A is incorrect. Monitor and Control Risk is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project. It can involve choosing alternative strategies, executing a contingency or fallback plan, taking corrective action, and modifying the project management plan.
Answer: D is incorrect. Qualitative analysis is the definition of risk factors in terms of high/medium/low or a numeric scale (1 to 10). Hence it determines the nature of risk on a relative scale.
Some of the qualitative methods of risk analysis are:

Scenario analysis- This is a forward-looking process that can reflect risk for a given point in time.
Risk Control Self -assessment (RCSA) - RCSA is used by enterprises (like banks) for the identification and evaluation of operational risk exposure. It is a logical first step and assumes that business owners and managers are closest to the issues and have the most expertise as to the source of the risk. RCSA is a constructive process in compelling business owners to contemplate, and then explain, the issues at hand with the added benefit of increasing their accountability.

QUESTION 51
Out of several risk responses, which of the following risk responses is used for negative risk events?

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

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Among the given choices only Acceptance response is used for negative risk events. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs. If an enterprise adopts a risk acceptance, it should carefully consider who can accept the risk. Risk should be accepted only by senior management in relationship with senior management and the board. There are two alternatives to the acceptance strategy, passive and active.
Passive acceptance means that enterprise has made no plan to avoid or mitigate the risk but willing to accept the consequences of the risk.
Active acceptance is the second strategy and might include developing contingency plans and reserves to deal with risks.
Answer: C, A, and B are incorrect. These all are used to deal with opportunities or positive risks, and not with negative risks.

QUESTION 52
Which of the following risks refer to probability that an actual return on an investment will be lower than the investor's expectations?

A. Integrity risk
B. Project ownership risk
C. Relevance risk
D. Expense risk

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:

Probability that an actual return on an investment will be lower than the investor's expectations is termed as investment risk or expense risk. All investments have some level of risk associated with it due to the unpredictability of the market's direction. This includes consideration of the overall IT investment portfolio. Answer: A is incorrect. The risk that data cannot be relied on because they are unauthorized, incomplete or inaccurate is termed as integrity risks. Answer: C is incorrect. The risk associated with not receiving the right information to the right people (or process or systems) at the right time to allow the right action to be taken is termed as relevance risk.
Answer: B is incorrect. The risk of IT projects failing to meet objectives due to lack of accountability and commitment is referring to as project risk ownership.

QUESTION 53
What are the PRIMARY requirements for developing risk scenarios? Each correct answer represents a part of the solution. Choose two.

A. Potential threats and vulnerabilities that could lead to loss events
B. Determination of the value of an asset at risk
C. Determination of actors that has potential to generate risk
D. Determination of threat type

Correct Answer: AB
Section: Volume A
Explanation

Explanation/Reference:
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: C and D are incorrect. Determination of actors and threat type are not the primary requirements for developing risk scenarios, but are the components that are determined during risk scenario development.

QUESTION 54
What are the responsibilities of the CRO?
Each correct answer represents a complete solution. Choose three.

A. Managing the risk assessment process

B. Implement corrective actions

C. Advising Board of Directors

D. Managing the supporting risk management function

Correct Answer: ABD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Chief Risk Officer is the executive-level manager in an organization. They provide corporate, guidance, governance, and oversight over the enterprise's risk management activities. The main priority for the CRO is to ensure that the organization is in full compliance with applicable regulations. They may also deal with areas regarding insurance, internal auditing, corporate investigations, fraud, and information security.
CRO's responsibilities include:
Managing the risk assessment process
Implementation of corrective actions
Communicate risk management issues
Supporting the risk management functions

QUESTION 55
You are working with a vendor on your project. A stakeholder has requested a change for the project, which will add value to the project deliverables. The vendor that you're working with on the project will be affected by the change. What system can help you introduce and execute the stakeholder change request with the vendor?

A. Contract change control system

B. Scope change control system

C. Cost change control system

D. Schedule change control system

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The contract change control system is part of the project's change control system. It addresses changes with the vendor that may affect the project contract.
Change control system, a part of the configuration management system, is a collection of formal documented procedures that define how project deliverables and documentation will be controlled, changed, and approved.
Answer: C is incorrect. The cost change control system manages changes to costs in the project.
Answer: D is incorrect. There is no indication that the change could affect the project schedule.

Answer: B is incorrect. The scope may change because of the stakeholder change request. Vendor's relationship to the project, hence this choice is not the best answer.

QUESTION 56
You are the project manager of GHT project. You are performing cost and benefit analysis of control. You come across the result that costs of specific controls exceed the benefits of mitigating a given risk. What is the BEST action would you choose in this scenario?

A. The enterprise may apply the appropriate control anyway.
B. The enterprise should adopt corrective control.
C. The enterprise may choose to accept the risk rather than incur the cost of mitigation.
D. The enterprise should exploit the risk.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
If the costs of specific controls or countermeasures (control overhead) exceed the benefits of mitigating a given risk the enterprise may choose to accept the risk rather than incur the cost of mitigation. This is done according to the principle of proportionality described in:
Generally accepted security systems principles (GASSP) Generally accepted information security principles (GAISP) Answer: A is incorrect. When the cost of specific controls exceed the benefits of mitigating a given risk, then controls are not applied, rather risk is being accepted. Answer: D is incorrect. The risk is being exploited when there is an opportunity, i.e., the risk is positive. But here in this case, negative risk exists as it needs mitigation. So, exploitation cannot be done.
Answer: B is incorrect. As the cost of control exceeds the benefits of mitigating a given risk, hence no control should be applied.
Corrective control is a type of control and hence it should not be adopted.

QUESTION 57
Mortality tables are based on what mathematical activity? Each correct answer represents a complete solution. Choose three.

A. Normal distributions
B. Probabilities
C. Impact
D. Sampling

Correct Answer: ABD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:

Probability identifies the chances that a particular event will happen under certain circumstances.
The variables provided are based on information gathered in real life. For situations with large numbers, a smaller set of participants are identified to represent the larger population. This represents a sample of the population. The points are mapped to identify their distribution.
Normal distribution refers to the theoretical plotting of points against the mathematical mean. The result of these activities provides a reasonable predictability for the mortality of the subject.
Answer: C is incorrect. Impact is used to identify the magnitude of identified risks. The risk leads to some type of loss. However, instead of quantifying the loss as a dollar value, an impact assessment could use words such as Low, Medium, or High. Hence it is not mathematical.

QUESTION 58
Harry is the project manager of HDW project. He has identified a risk that could injure project team members. He does not want to accept any risk where someone could become injured on this project so he hires a professional vendor to complete this portion of the project work. What type of risk response is Harry implementing?

A. Transference
B. Mitigation
C. Acceptance
D. Avoidance

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Risk transfer means that impact of risk is reduced by transferring or otherwise sharing a portion of the risk with an external organization or another internal entity. Transfer of risk can occur in many forms but is most effective when dealing with financial risks. Insurance is one form of risk transfer. Hence when Harry hires a professional vendor to manage that risk, the risk event does not go away but the responsibility for the event is transferred to the vendor.
Answer: D is incorrect. Avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope. Answer: C is incorrect. Mitigation are actions that Harry's project team could take to reduce the probability and/or impact of a risk event.
Answer: B is incorrect. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs. Here
Harry is not accepting this risk event; he does not want anyone of his team to become injured so he's transferring the event to professional vendor.

QUESTION 59
The Identify Risk process determines the risks that affect the project and document their characteristics. Why should the project team members be involved in the Identify Risk process?

A. They are the individuals that will most likely cause and respond to the risk events.
B. They are the individuals that will have the best responses for identified risks events within the project.
C. They are the individuals that are most affected by the risk events.
D. They are the individuals that will need a sense of ownership and responsibility for the risk events.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The project team members should be involved in the risk identification so that they will develop a sense of ownership and responsibility for the risk events and the associated risk responses.
Identify Risks is the process of determining which risks may affect the project. It also documents risks' characteristics. The Identify Risks process is part of the Project Risk Management knowledge area. As new risks may evolve or become known as the project progresses through its life cycle, Identify Risks is an iterative process. The process should involve the project team so that they can develop and maintain a sense of ownership and responsibility for the risks and associated risk response actions. Risk Register is the only output of this process.
Answer: C, B, and A are incorrect. These are not the valid answers for this QUESTION NO:

QUESTION 60
What are the requirements of monitoring risk?
Each correct answer represents a part of the solution. Choose three.

A. Information of various stakeholders
B. Preparation of detailed monitoring plan
C. Identifying the risk to be monitored
D. Defining the project's scope

Correct Answer: BCD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
It is important to first understand the risk to be monitored, prepare a detailed plan and define the project's scope for monitoring risk. In the case of a monitoring project, this step should involve process owners, data owners, system custodians and other process stakeholders. Answer: A is incorrect. Data regarding stakeholders of the project is not required in any phase of risk monitoring.

QUESTION 61
Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

A. Risk transfer
B. Risk acceptance

C. Risk avoidance
D. Risk mitigation

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Risk transfer is the practice of passing risk from one entity to another entity. In other words, if a company is covered under a liability insurance policy providing various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc., it means it has transferred its security risks to the insurance company. Answer: D is incorrect. Risk mitigation is the practice of reducing the severity of the loss or the likelihood of the loss from occurring. Answer: C is incorrect. Risk avoidance is the practice of not performing an activity that could carry risk. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Answer: B is incorrect. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

QUESTION 62
You work as a project manager for BlueWell Inc. Management has asked you to work with the key project stakeholder to analyze the risk events you have identified in the project. They would like you to analyze the project risks with a goal of improving the project's performance as a whole. What approach can you use to achieve this goal of improving the project's performance through risk analysis with your project stakeholders?

A. Involve subject matter experts in the risk analysis activities
B. Involve the stakeholders for risk identification only in the phases where the project directly affects them
C. Use qualitative risk analysis to quickly assess the probability and impact of risk events
D. Focus on the high-priority risks through qualitative risk analysis

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
By focusing on the high-priority of risk events through qualitative risk analysis you can improve the project's performance.
Qualitative analysis is the definition of risk factors in terms of high/medium/low or a numeric scale (1 to 10). Hence it determines the nature of risk on a relative scale. Some of the qualitative methods of risk analysis are:
Scenario analysis- This is a forward-looking process that can reflect risk for a given point in time.
Risk Control Self -assessment (RCSA) - RCSA is used by enterprises (like banks) for the identification and evaluation of operational risk exposure. It is a logical first step and assumes that business owners and managers are closest to the issues and have the most expertise as to the source of the risk. RCSA is a constructive process in compelling business owners to contemplate, and then explain, the issues at hand with the added benefit of increasing their accountability.
Answer: A is incorrect. Subject matter experts can help the qualitative risk assessment, but by focusing on high-priority risks the project's performance can improve

by addressing these risk events.
Answer: B is incorrect. Stakeholders should be involved throughout the project as situations within the project demand their input to risk identification and analysis.
Answer: C is incorrect. Qualitative analysis does use a fast approach of analyzing project risks, but it's not the best answer for this

QUESTION 63
You are a project manager for your organization and you're working with four of your key stakeholders. One of the stakeholders is confused as to why you're not discussing the current problem in the project during the risk identification meeting. Which one of the following statements best addresses when a project risk actually happens?

A. Project risks are uncertain as to when they will happen.
B. Risks can happen at any time in the project.
C. Project risks are always in the future.
D. Risk triggers are warning signs of when the risks will happen.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
According to the PMBOK, a project risk is always in the future. If the risk event has already happened, then it is an issue, not a risk.
Answer: A is incorrect. You can identify risks before they occur and not after their occurrence.
Answer: D is incorrect. Triggers are warning signs and conditions of risk events, but this answer isn't the best choice for this option B is incorrect. Risks can only happen in the future.

QUESTION 64
Which of the following is the MOST effective method for indicating that the risk level is approaching a high or unacceptable level of risk?

A. Risk register
B. Cause and effect diagram
C. Risk indicator
D. Return on investment

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Risk indicators are metrics used to indicate risk thresholds, i.e., it gives indication when a risk level is approaching a high or unacceptable level of risk. The main

objective of a risk indicator is to ensure tracking and reporting mechanisms that alert staff about the potential risks.
Answer: D is incorrect. Return On Investment (ROI) is a performance measure used to evaluate the efficiency of an investment or to compare the efficiency of a number of different investments. To calculate ROI, the benefit (return) of an investment is divided by the cost of the investment; the result is expressed as a percentage or a ratio.
The return on investment formula:
ROI= (Gain from investment - Cost of investment) / Cost of investment In the above formula "gains from investment", refers to the proceeds obtained from selling the investment of interest.
Answer: A is incorrect. A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains:
A description of the risk
The impact should this event actually occur
The probability of its occurrence
Risk Score (the multiplication of Probability and Impact) A summary of the planned response should the event occur A summary of the mitigation (the actions taken in advance to reduce the probability and/or impact of the event)
Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved.

QUESTION 65
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. Risk Management Plan
B. Stakeholder management strategy
C. Communications Management Plan
D. Resource Management Plan

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
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: B is incorrect. The stakeholder management strategy does not address risk communications.
Answer: A is incorrect. The Risk Management Plan defines risk identification, analysis, response, and monitoring.
Answer: D is incorrect. The Resource Management Plan does not define risk communications.

QUESTION 66

Your project spans the entire organization. You would like to assess the risk of your project but worried about that some of the managers involved in the project could affect the outcome of any risk identification meeting. Your consideration is based on the fact that some employees would not want to publicly identify risk events that could declare their supervision as poor. You would like a method that would allow participants to anonymously identify risk events. What risk identification method could you use?

A. Delphi technique
B. Root cause analysis
C. Isolated pilot groups
D. SWOT analysis

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The Delphi technique uses rounds of anonymous surveys to build consensus on project risks. Delphi is a technique to identify potential risk. In this technique, the responses are gathered via a question and their inputs are organized according to their contents. The collected responses are sent back to these experts for further input, addition, and comments. The final list of risks in the project is prepared after that. The participants in this technique are anonymous and therefore it helps prevent a person from unduly influencing the others in the group. The Delphi technique helps in reaching the consensus quickly. Answer: C is incorrect. Isolated pilot groups is not a valid risk identification activity. Answer: B is incorrect. Root cause analysis is not an anonymous approach to risk identification.
Answer: D is incorrect. SWOT analysis evaluates the strengths, weaknesses, opportunities, and threats of the project.

QUESTION 67
Which of the following represents lack of adequate controls?

A. Vulnerability
B. Threat
C. Asset
D. Impact

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Vulnerability is a weakness or lack of safeguard that can be exploited by a threat, thus causing harm to the information systems or networks. It can exist in hardware, operating systems, firmware, applications, and configuration files. Hence lack of adequate controls represents vulnerability and would ultimately cause threat to the enterprise. Answer: B is incorrect. Threat is the potential cause of unwanted incident. Answer: D is incorrect. Impact is the measure of the financial

loss that the threat event may have.
Answer: C is incorrect. Assets are economic resources that are tangible or intangible, and is capable of being owned or controlled to produce value.

QUESTION 68
The only output of qualitative risk analysis is risk register updates. When the project manager updates the risk register he will need to include several pieces of information including all of the following except for which one?

A. Trends in qualitative risk analysis
B. Risk probability-impact matrix
C. Risks grouped by categories
D. Watchlist of low-priority risks

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The risk matrix is not included as part of the risk register updates. There are seven things that can be updated in the risk register as a result of qualitative risk analysis: relating ranking of project risks, risks grouped by categories, causes of risks, list of near-term risks, risks requiring additional analysis, watchlist of low-priority risks, trends in qualitative risk analysis.
Answer: C is incorrect. Risks grouped by categories are part of the risk register updates. Answer: D is incorrect. Watchlist of low-priority risks is part of the risk register updates. Answer: A is incorrect. Trends in qualitative risk analysis are part of the risk register updates.

QUESTION 69
Which of the following risks is the risk that happen with an important business partner and affects a large group of enterprises within an area or industry?

A. Contagious risk
B. Reporting risk
C. Operational risk
D. Systemic risk

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Systemic risks are those risks that happen with an important business partner and affect a large group of enterprises within an area or industry. An example would be a nationwide air traffic control system that goes down for an extended period of time (six hours), which affects air traffic on a very large scale.

Answer: A is incorrect. Contagious risks are those risk events that happen with several of the enterprise's business partners within a very short time frame. Answer: C and B are incorrect. Their scopes do not limit to the important or general enterprise's business partners. These risks can occur with both. Operational risks are those risks that are associated with the day-to-day operations of the enterprise. It is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.
Reporting risks are caused due to wrong reporting which leads to bad decision. This bad decision due to wrong report hence causes a risk on the functionality of the organization.

QUESTION 70
You have been assigned as the Project Manager for a new project that involves development of a new interface for your existing time management system. You have completed identifying all possible risks along with the stakeholders and team and have calculated the probability and impact of these risks. Which of the following would you need next to help you prioritize the risks?

A. Affinity Diagram
B. Risk rating rules
C. Project Network Diagram
D. Risk categories

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Risk rating rules define how to prioritize risks after the related probability and impact values are calculated. These are generally included in the organizational process assets and are refined for individual projects.
Answer: A is incorrect. Affinity Diagram is a method of group creativity technique to collect requirements which allows large numbers of ideas to be sorted into groups for review and analysis. This is generally used in Scope Management and not applicable to this option D is incorrect. Risk categories are an output of the Perform Qualitative Risk Analysis process and not a tool to complete the process.
Answer: C is incorrect. A Project Network diagram shows the sequencing and linkage between various project tasks and is not applicable to this

QUESTION 71
You are the project manager of a large networking project. During the execution phase the customer requests for a change in the existing project plan. What will be your immediate action?

A. Update the risk register.
B. Ask for a formal change request.
C. Ignore the request as the project is in the execution phase.
D. Refuse the change request.

Correct Answer: B

Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Whenever the customer or key stakeholder asks for a change in the existing plan, you should ask him/her to submit a formal change request. Change requests may modify project policies or procedures, project scope, project cost or budget, project schedule, or project quality. Answer: C, A, and D are incorrect. The first action required is to create a formal change request, if a change is requested in the project.

QUESTION 72
Which of the following is described by the definition given below? "It is the expected guaranteed value of taking a risk."

A. Certainty equivalent value
B. Risk premium
C. Risk value guarantee
D. Certain value assurance

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The Certainty equivalent value is the expected guaranteed value of taking a risk. It is derived by the uncertainty of the situation and the potential value of the situation's outcome. Answer: B is incorrect. The risk premium is the difference between the larger expected value of the risk and the smaller certainty equivalent value. Answer: and are incorrect. These are not valid answers.

QUESTION 73
You are the project manager of GHT project. Your hardware vendor left you a voicemail saying that the delivery of the equipment you have ordered would not arrive on time. She wanted to give you a heads-up and asked that you return the call. Which of the following statements is TRUE?

A. This is a residual risk.
B. This is a trigger.
C. This is a contingency plan.
D. This is a secondary risk.

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Triggers are warning signs of an upcoming risk event. Here delay in delivery signifies that there may be a risk event like delay in completion of project. Hence it is referred to as a trigger.
Answer: C is incorrect. A contingency plan is a plan devised for a specific situation when things go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen.
Here there are no such plans.
Answer: A is incorrect. Residual risk is the risk that remains after applying controls. But here in this scenario, risk event has not occurred yet.
Answer: D is incorrect. Secondary risks are risks that come about as a result of implementing a risk response. But here in this scenario, risk event has not occurred yet.

QUESTION 74
There are five inputs to the quantitative risk analysis process. Which one of the following is NOT an input to quantitative risk analysis process?

A. Risk management plan
B. Enterprise environmental factors
C. Cost management plan
D. Risk register

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Enterprise environmental factor is not an input to the quantitative risk analysis process. The five inputs to the perform quantitative risk analysis process are: risk register, risk management plan, cost management plan, schedule management plan, and organizational process assets.
Answer: D, A, and C are incorrect. These are the valid inputs to the perform quantitative risk analysis process.

QUESTION 75
Stephen is the project manager of the GBB project. He has worked with two subject matter experts and his project team to complete the risk assessment technique. There are approximately 47 risks that have a low probability and a low impact on the project. Which of the following answers best describes what Stephen should do with these risk events?

A. Because they are low probability and low impact, Stephen should accept the risks.
B. The low probability and low impact risks should be added to a watchlist for future monitoring.
C. Because they are low probability and low impact, the risks can be dismissed.
D. The low probability and low impact risks should be added to the risk register.

Correct Answer: B

Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The low probability and low impact risks should be added to a watchlist for future monitoring.
Answer: A is incorrect. The risk response for these events may be to accept them, but the best answer is to first add them to a watchlist.
Answer: C is incorrect. Risks are not dismissed; they are at least added to a watchlist for monitoring.
Answer: D is incorrect. While the risks may eventually be added to the register, the best answer is to first add them to the watchlist for monitoring.

QUESTION 76
Jenny is the project manager for the NBT projects. She is working with the project team and several subject matter experts to perform the quantitative risk analysis process. During this process she and the project team uncover several risks events that were not previously identified. What should Jenny do with these risk events?

A. The events should be entered into qualitative risk analysis.
B. The events should be determined if they need to be accepted or responded to.
C. The events should be entered into the risk register.
D. The events should continue on with quantitative risk analysis.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
All identified risk events should be entered into the risk register. A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains:
A description of the risk
The impact should this event actually occur
The probability of its occurrence
Risk Score (the multiplication of Probability and Impact) A summary of the planned response should the event occur A summary of the mitigation (the actions taken in advance to reduce the probability and/or impact of the event)
Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved. Answer: A is incorrect. Before the risk events are analyzed they should be documented in the risk register.
Answer: D is incorrect. These risks should first be identified, documented, passed through qualitative risk analysis and then it should be determined if they should pass through the quantitative risk analysis process.
Answer: B is incorrect. The risks should first be documented and analyzed.

QUESTION 77
You are working on a project in an enterprise. Some part of your project requires e- commerce, but your enterprise choose not to engage in e-commerce. This

scenario is demonstrating which of the following form?

A. risk avoidance
B. risk treatment
C. risk acceptance
D. risk transfer

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Each business process involves inherent risk. Not engaging in any activity avoids the inherent risk associated with the activity. Hence this demonstrates risk avoidance. Answer: D is incorrect. Risk transfer/sharing means reducing either risk frequency or impact by transferring or otherwise sharing a portion of the risk. Common techniques include insurance and outsourcing. These techniques do not relieve an enterprise of a risk, but can involve the skills of another party in managing the risk and reducing the financial consequence if an adverse event occurs.
Answer: B is incorrect. Risk treatment means that action is taken to reduce the frequency and impact of a risk.
Answer: C is incorrect. Acceptance means that no action is taken relative to a particular risk, and loss is accepted when/if it occurs. This is different from being ignorant of risk; accepting risk assumes that the risk is known, i.e., an informed decision has been made by management to accept it as such.

QUESTION 78
Which of the following are risk components of the COSO ERM framework? Each correct answer represents a complete solution. Choose three.

A. Risk response
B. Internal environment
C. Business continuity
D. Control activities

Correct Answer: ABD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The risk components defined by the COSO ERM are internal environment, objective settings, event identification, risk assessment, risk response, control objectives, information and communication, and monitoring.
Answer: C is incorrect. Business continuity is not considered as risk component within the ERM framework.

QUESTION 79

Your project team has completed the quantitative risk analysis for your project work. Based on their findings, they need to update the risk register with several pieces of information. Which one of the following components is likely to be updated in the risk register based on their analysis?

A. Listing of risk responses
B. Risk ranking matrix
C. Listing of prioritized risks
D. Qualitative analysis outcomes

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The outcome of quantitative analysis can create a listing of prioritized risks that should be updated in the risk register. The project team will create and update the risk register with four key components: probabilistic analysis of the project, probability of achieving time and cost objectives, list of quantified risks, and trends in quantitative risk analysis. Answer: D, B, and A are incorrect. These subjects are not updated in the risk register as a result of quantitative risk analysis.

QUESTION 80
Fred is the project manager of a large project in his organization. Fred needs to begin planning the risk management plan with the project team and key stakeholders. Which plan risk management process tool and technique should Fred use to plan risk management?

A. Information gathering techniques
B. Data gathering and representation techniques
C. Planning meetings and analysis
D. Variance and trend analysis

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
There is only one tool and technique available for Fred to plan risk management: planning meetings and analysis. Planning Meeting and Analysis is a tool and technique in the Plan Risk Management process. Planning meetings are organized by the project teams to develop the risk management plan. Attendees at these meetings include the following:
Project manager
Selected project team members
Stakeholders
Anybody in the organization with the task to manage risk planning Sophisticated plans for conducting the risk management activities are defined in these meetings,

responsibilities related to risk management are assigned, and risk contingency reserve application approaches are established and reviewed.
Answer: A, D, and B are incorrect. These are not plan risk management tools and techniques.

QUESTION 81
Which of the following is the HIGHEST risk of a policy that inadequately defines data and system ownership?

A. User management coordination does not exists
B. Audit recommendations may not be implemented
C. Users may have unauthorized access to originate, modify or delete data
D. Specific user accountability cannot be established

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
There is an increased risk without a policy defining who has the responsibility for granting access to specific data or systems, as one could gain system access without a justified business needs. There is better chance that business objectives will be properly supported when there is appropriate ownership.
Answer: A, B, and D are incorrect. These risks are not such significant as compared to unauthorized access.

QUESTION 82
Marie has identified a risk event in her project that needs a mitigation response. Her response actually creates a new risk event that must now be analyzed and planned for. What term is given to this newly created risk event?

A. Residual risk
B. Secondary risk
C. Infinitive risk
D. Populated risk

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Secondary risks are the risks that come about as a result of implementing a risk response. This new risk event must be recorded, analyzed, and planned for management. Answer: A is incorrect. A residual risk event is similar to a secondary risk, but is often small in probability and impact, so it may just be accepted.
Answer: D is incorrect. Populated risk event is not a valid project management term. Answer: C is incorrect. Infinitive risk is not a valid project management term.

QUESTION 83
Which one of the following is the only output for the qualitative risk analysis process?

A. Project management plan
B. Risk register updates
C. Organizational process assets
D. Enterprise environmental factors

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Risk register update is the only output of the choices presented for the qualitative risk analysis process. The four inputs for the qualitative risk analysis process are the risk register, risk management plan, project scope statement, and organizational process assets. The output of perform qualitative risk analysis process is Risk Register Updates. Risk register is updated with the information from perform qualitative risk analysis and the updated risk register is included in the project documents. Updates include the following important elements:
Relative ranking or priority list of project risks
Risks grouped by categories
Causes of risk or project areas requiring particular attention List of risks requiring response in the near-term
List of risks for additional analysis and response
Watchlist of low priority risks
Trends in qualitative risk analysis results
Answer: C, D, and A are incorrect. These are not the valid outputs for the qualitative risk analysis process.

QUESTION 84
FISMA requires federal agencies to protect IT systems and data. How often should compliance be audited by an external organization?

A. Annually
B. Quarterly
C. Every three years
D. Never

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:

Inspection of FISMA is required to be done annually. Each year, agencies must have an independent evaluation of their program. The objective is to determine the effectiveness of the program. These evaluations include:
Testing for effectiveness: Policies, procedures, and practices are to be tested. This evaluation does not test every policy, procedure, and practice. Instead, a representative sample is tested. An assessment or report: This report identifies the agency's compliance as well as lists compliance with FISMA. It also lists compliance with other standards and guidelines. Answer: D, B, and C are incorrect. Auditing of compliance by external organization is done annually, not quarterly or every three year.

QUESTION 85
Which of the following is the FOREMOST root cause of project risk? Each correct answer represents a complete solution. Choose two.

A. New system is not meeting the user business needs
B. Delay in arrival of resources
C. Lack of discipline in managing the software development process
D. Selection of unsuitable project methodology

Correct Answer: CD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The foremost root cause of project risk is:
A lack of discipline in managing the software development process Selection of a project methodology that is unsuitable to the system being developed Answer: A is incorrect. The risk associated with new system is not meeting the user business needs is business risks, not project risk.
Answer: B is incorrect. This is not direct reason of project risk.

QUESTION 86
You are the project manager of a SGT project. You have been actively communicating and working with the project stakeholders. One of the outputs of the "manage stakeholder expectations" process can actually create new risk events for your project. Which output of the manage stakeholder expectations process can create risks?

A. Project management plan updates
B. An organizational process asset updates
C. Change requests
D. Project document updates

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The manage stakeholder expectations process can create change requests for the project, which can cause new risk events to enter into the project. Change requests are requests to expand or reduce the project scope, modify policies, processes, plans, or procedures, modify costs or budgets or revise schedules. These requests for a change can be direct or indirect, externally or internally initiated, and legally or contractually imposed or optional. A Project Manager needs to ensure that only formally documented requested changes are processed and
only approved change requests are implemented.
Answer: A is incorrect. The project management plan updates do not create new risks. Answer: D is incorrect. The project document updates do not create new risks. Answer: B is incorrect. The organizational process assets updates do not create new risks.

QUESTION 87
Which of the following characteristics of risk controls can be defined as under? "The separation of controls in the production environment rather than the separation in the design and implementation of the risk"

A. Trusted source
B. Secure
C. Distinct
D. Independent

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
A control or countermeasure which does not overlap in its performance with another control or countermeasure is considered as distinct.
Hence the separation of controls in the production environment rather than the separation in the design and implementation of the risk refers to distinct. Answer: D is incorrect. The separation in design, implementation, and maintenance of controls or countermeasures are refer to as independent. Hence this answer is not valid. Answer: B is incorrect. Secure controls refers to the activities ability to protect from exploitation or attack.
Answer: A is incorrect. Trusted source refers to the commitment of the people designing, implementing, and maintenance of the control towards the security policy.

QUESTION 88
Shelly is the project manager of the BUF project for her company. In this project Shelly needs to establish some rules to reduce the influence of risk bias during the qualitative risk analysis process. What method can Shelly take to best reduce the influence of risk bias?

A. Establish risk boundaries
B. Group stakeholders according to positive and negative stakeholders and then complete the risk analysis
C. Determine the risk root cause rather than the person identifying the risk events
D. Establish definitions of the level of probability and impact of risk event

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
By establishing definitions for the level of probability and impact a project manager can reduce the influence of bias.
Answer: A is incorrect. This is not a valid statement for reducing bias in the qualitative risk analysis.
Answer: B is incorrect. Positive and negative stakeholders are identified based on their position towards the project goals and objectives, not necessarily risks.
Answer: C is incorrect. Root cause analysis is a good exercise, but it would not determine risk bias.

QUESTION 89
You are the IT manager in Bluewell Inc. You identify a new regulation for safeguarding the information processed by a specific type of transaction. What would be the FIRST action you will take?

A. Assess whether existing controls meet the regulation
B. Update the existing security privacy policy
C. Meet with stakeholders to decide how to comply
D. Analyze the key risk in the compliance process

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
When a new regulation for safeguarding information processed by a specific type of transaction is being identified by the IT manager, then the immediate step would be to understand the impact and requirements of this new regulation. This includes assessing how the enterprise will comply with the regulation and to what extent the existing control structure supports the compliance process. After that manager should then assess any existing gaps. Answer: D, C, and B are incorrect. These choices are appropriate as well as important, but are subsequent steps after understanding and gap assessment.

QUESTION 90
You are the risk official of your enterprise. You have just completed risk analysis process. You noticed that the risk level associated with your project is less than risk tolerance level of your enterprise. Which of following is the MOST likely action you should take?

A. Apply risk response
B. Update risk register
C. No action
D. Prioritize risk response options

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
When the risk level is less than risk tolerance level of the enterprise than no action is taken against that, because the cost of mitigation will increase over its benefits. Answer: D is incorrect. This is not valid answer, as no response is being applied to such low risk level.
Answer: B is incorrect. Risk register is updates after applying response, and as no response is applied to such low risk level; hence no updating is done. Answer: A is incorrect. This is not valid answer, as no response is being applied to such low risk level.

QUESTION 91
Which of the following operational risks ensures that the provision of a quality product is not overshadowed by the production costs of that product?

A. Information security risks
B. Contract and product liability risks
C. Project activity risks
D. Profitability operational risks

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Profitability operational risks focus on the financial risks which encompass providing a quality product that is cost-effective in production. It ensures that the provision of a quality product is not overshadowed by the production costs of that product. Answer: A is incorrect. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security risks are the risks that are associated with the protection of these information and information systems. Answer: C is incorrect. Project activity risks are not associated with provision of a quality product or the production costs of that product.
Answer: B is incorrect. These risks do not ensure that the provision of a quality product is not overshadowed by the production costs of that product.

QUESTION 92
Which of the following is the process of numerically analyzing the effects of identified risks on the overall enterprise's objectives?

A. Identifying Risks
B. Quantitative Risk Assessment
C. Qualitative Risk Assessment
D. Monitoring and Controlling Risks

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
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.
Answer: C is incorrect.
Unlike the quantitative risk assessment, qualitative risk assessment does not assign dollar values. Rather, it determines risk's level based on the probability and impact of a risk. These values are determined by gathering the opinions of experts. Probability- establishing the likelihood of occurrence and reoccurrence of specific risks, independently, and combined. The risk occurs when a threat exploits vulnerability. Scaling is done to define the probability that a risk will occur. The scale can be based on word values such as Low, Medium, or High. Percentage can also be assigned to these words, like 10% to low and 90% to high.
Impact- Impact is used to identify the magnitude of identified risks. The risk leads to some type of loss. However, instead of quantifying the loss as a dollar value, an impact assessment could use words such as Low, Medium, or High. Impact is expressed as a relative value. For example, low could be 10, medium could be 50, and high could be 100.
Risk level= Probability*Impact
Answer: A is incorrect.
The first thing we must do in risk management is to identify the areas of the project where the risks can occur. This is termed as risk identification. Listing all the possible risks is proved to be very productive for the enterprise as we can 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. This is the process of implementing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness through the project.

QUESTION 93
Which of the following processes is described in the statement below? "It is the process of exchanging information and views about risks among stakeholders, such as groups, individuals, and institutions."

A. Risk governance
B. IRGC
C. Risk response planning

D. Risk communication

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Risk communication is the process of exchanging information and views about risks among stakeholders, such as groups, individuals, and institutions. Risk communication is mostly concerned with the nature of risk or expressing concerns, views, or reactions to risk managers or institutional bodies for risk management. The key plan to consider and communicate risk is to categorize and impose priorities, and acquire suitable measures to reduce risks. It is important throughout any crisis to put across multifaceted information in a simple and clear manner. Risk communication helps in switching or allocating the information concerning risk among the decision-maker and the stakeholders. Risk communication can be explained more clearly with the help of the following definitions:
It defines the issue of what a group does, not just what it says. It must take into account the valuable element in user's perceptions of risk. It will be more valuable if it is thought of as conversation, not instruction. Risk communication is a fundamental and continuing element of the risk analysis exercise, and the involvement of the stakeholder group is from the beginning. It makes the stakeholders conscious of the process at each phase of the risk assessment. It helps to guarantee that the restrictions, outcomes, consequence, logic, and risk assessment are undoubtedly understood by all the stakeholders.
Answer: C is incorrect. Risk response is a process of deciding what measures should be taken to reduce threats and take advantage of the opportunities discovered during the risk analysis processes. This process also includes assigning departments or individual staff members the responsibility of carrying out the risk response plans and these folks are known as risk owners.
The prioritization of the risk responses and development of the risk response plan is based on following parameters:
Cost of the response to reduce risk within tolerance levels Importance of the risk
Capability to implement the response
Effectiveness and efficiency of the response
Risk prioritization strategy is used to create a risk response plan and implementation schedule because all risk cannot be addressed at the same time. It may take considerable investment of time and resources to address all the risk identified in the risk analysis process. Risk with a greater likelihood and impact on the enterprise will prioritized above other risk that is considered less likely or lay less impact.
Answer: A is incorrect. Risk governance is a systemic approach to decision making processes associated to natural and technological risks. It is based on the principles of cooperation, participation, mitigation and sustainability, and is adopted to achieve more effective risk management. It seeks to reduce risk exposure and vulnerability by filling gaps in risk policy, in order to avoid or reduce human and economic costs caused by disasters. Risk governance is a continuous life cycle that requires regular reporting and ongoing review. The risk governance function must oversee the operations of the risk management team. Answer: B is incorrect. The International Risk Governance Council (IRGC) is a self- governing organization whose principle is to facilitate the understanding and managing the rising overall risks that have impacts on the economy and society, human health and safety, the environment at large. IRGC's effort is to build and develop concepts of risk governance, predict main risk issues and present risk governance policy recommendations for the chief decision makers. IRGC mainly emphasizes on rising, universal risks for which governance deficits exist.
Its goal is to present recommendations for how policy makers can correct them. IRGC models at constructing strong, integrative inter-disciplinary governance models for up- coming and existing risks.

QUESTION 94
Which of the following are the principles of risk management? Each correct answer represents a complete solution. Choose three.

A. Risk management should be an integral part of the organization

B. Risk management should be a part of decision-making

C. Risk management is the responsibility of executive management

D. Risk management should be transparent and inclusive

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The International Organization for Standardization (ISO) identifies the following principles of risk management. Risk management should:
create value
be an integral part of organizational processes
be part of decision making
explicitly address uncertainty
be systematic and structured
be based on the best available information
be tailored
take into account human factors
be transparent and inclusive
be dynamic, iterative, and responsive to change
be capable of continual improvement and enhancement

QUESTION 95
Which of the following characteristics of risk controls answers the aspect about the control given below: "Will it continue to function as expressed over the time and adopts as changes or new elements are introduced to the environment"

A. Reliability

B. Sustainability

C. Consistency

D. Distinct

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Sustainability ensures that the control continues to function as expressed over the time and adopts as changes or new elements are introduced to the environment.
Answer: C is incorrect. Consistent characteristic of the control tells whether the control can be applied in the same manner across the organization. Answer: A is

incorrect. Reliability of control ensures that it will serve its purpose under multiple circumstances.
Answer: D is incorrect. A control or countermeasure which does not overlap in its performance with another control or countermeasure is considered as distinct. Hence the separation of controls in the production environment rather than the separation in the design and implementation of the risk refers to distinct.

QUESTION 96
Jeff works as a Project Manager for www.company.com Inc. He and his team members are involved in the identify risk process. Which of the following tools & techniques will Jeff use in the identify risk process? Each correct answer represents a complete solution. Choose all that apply.

A. Information gathering technique
B. Documentation reviews
C. Checklist analysis
D. Risk categorization

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The various tools & techniques used in the identify risk process are as follows:
Documentation reviews
Information gathering technique
Checklist analysis
Assumption analysis
Diagramming techniques
SWOT analysis
Expert judgment

QUESTION 97
Mary is the project manager for the BLB project. She has instructed the project team to assemble, to review the risks. She has included the schedule management plan as an input for the quantitative risk analysis process. Why is the schedule management plan needed for quantitative risk analysis?

A. Mary will schedule when the identified risks are likely to happen and affect the project schedule.
B. Mary will utilize the schedule controls and the nature of the schedule for the quantitative analysis of the schedule.
C. Mary will use the schedule management plan to schedule the risk identification meetings throughout the remaining project.
D. Mary will utilize the schedule controls to determine how risks may be allowed to change the project schedule.

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The controls within the schedule management plan can shape how quantitative risk analysis will be performed on the schedule.
Schedule management plan also describes how the schedule contingencies will be reported and assessed.
Answer: C is incorrect. This is not a valid answer for this question throughout the project, but it is not scheduled during the quantitative risk analysis process.
Answer: A is incorrect. When risks are likely to happen is important, but it is not the best answer for this question option D is incorrect. Risks may affect the project schedule, but this is not the best answer for the question.

QUESTION 98
Which of the following control detects problem before it can occur?

A. Deterrent control
B. Detective control
C. Compensation control
D. Preventative control

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Preventative controls are the controls that detect the problem before it occurs. They attempt to predict potential problems and make adjustments to prevent those problems to occur in near future. This prediction is being made by monitoring both the system's operations and its inputs.
Answer: A is incorrect. Deterrent controls are similar to the preventative controls, but they diminish or reverse the attraction of the environment to prevent risk from occurring instead of making adjustments to the environment.
Answer: C is incorrect. Compensation controls ensure that normal business operations continue by applying appropriate resource.
Answer: B is incorrect. Detective controls simply detect and report on the occurrence of a problems. They identify specific symptoms to potential problems.

QUESTION 99
Which of the following aspects are included in the Internal Environment Framework of COSO ERM?
Each correct answer represents a complete solution. Choose three.

A. Enterprise's integrity and ethical values
B. Enterprise's working environment
C. Enterprise's human resource standards
D. Enterprise's risk appetite

Correct Answer: ACD

Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The internal environment for risk management is the foundational level of the COSO ERM framework, which describes the philosophical basics of managing risks within the implementing enterprise. The different aspects of the internal environment include the enterprise's:
Philosophy on risk management
Risk appetite
Attitudes of Board of Directors
Integrity and ethical values
Commitment to competence
Organizational structure
Authority and responsibility
Human resource standards

QUESTION 100
Which of the following type of risk could result in bankruptcy?

A. Marginal
B. Negligible
C. Critical
D. Catastrophic

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Catastrophic risk causes critical financial losses that have the possibility of bankruptcy. Answer: C is incorrect. Critical risk causes serious financial losses in more than one line of business with a loss in productivity.
Answer: A is incorrect. Marginal risk causes financial loss in a single line of business and a reduced return on IT investment.
Answer: B is incorrect. It causes minimal impact on a single line of business affecting their ability to deliver services or products.

QUESTION 101
Risks with low ratings of probability and impact are included for future monitoring in which of the following?

A. Risk alarm
B. Observation list

C. Watch-list

D. Risk register

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Watch-list contains risks with low rating of probability and impact. This list is useful for future monitoring of low risk factors.
Answer: D is incorrect. Risk register is a document that contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning. Description, category, cause, probability of occurring, impact on objectives, proposed responses, owner, and the current status of all identified risks are put in the risk register. Answer: A and B are incorrect. No such documents as risk alarm and observation list is prepared during risk identification process.

QUESTION 102
You are the project manager of your project. You have to analyze various project risks. You have opted for quantitative analysis instead of qualitative risk analysis. What is the MOST significant drawback of using quantitative analysis over qualitative risk analysis?

A. lower objectivity

B. higher cost

C. higher reliance on skilled personnel

D. lower management buy-in

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Quantitative risk analysis is generally more complex and thus is costlier than qualitative risk analysis.
Answer: A is incorrect. Neither of the two risk analysis methods is fully objective. Qualitative method subjectively assigns high, medium and low frequency and impact categories to a specific risk, whereas quantitative method subjectivity expressed in mathematical "weights".
Answer: C is incorrect. To be effective, both processes require personnel who have a good understanding of the business. So there is equal requirement of skilled personnel in both. Answer: D is incorrect. Quantitative analysis generally has a better buy-in than qualitative analysis to the point where it can cause over-reliance on the results. Hence this option is not correct.

QUESTION 103
You are working as the project manager of the ABS project. The project is for establishing a computer network in a school premises. During the project execution, the school management asks to make the campus Wi-Fi enabled. You know that this may impact the project adversely. You have discussed the change request with other stakeholders. What will be your NEXT step?

A. Update project management plan.
B. Issue a change request.
C. Analyze the impact.
D. Update risk management plan.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The first step after receiving any change request in a project must be first analyzed for its impact. Changes may be requested by any stakeholder involved with the project. Although, they may be initiated verbally, they should always be recorded in written form and entered into the change management and/or configuration management. Answer: A, B, and D are incorrect. All these are the required steps depending on the change request. Any change request must be followed by the impact analysis of the change.

QUESTION 104
Which of the following role carriers are responsible for setting up the risk governance process, establishing and maintaining a common risk view, making risk-aware business decisions, and setting the enterprise's risk culture? Each correct answer represents a complete solution. Choose two.

A. Senior management
B. Chief financial officer (CFO)
C. Human resources (HR)
D. Board of directors

Correct Answer: AD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The board of directors and senior management has the responsibility to set up the risk governance process, establish and maintain a common risk view, make risk-aware business decisions, and set the enterprise's risk culture.
Answer: B is incorrect. CFO is the most senior official 0f the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks. CFO is not responsible for responsible for setting up the risk governance process, establishing and maintaining a common risk view, making risk-aware business decisions, and setting the enterprise's risk culture.
Answer: C is incorrect. Human resource is the most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise.
HR is not responsible for risk related activities.

QUESTION 105
You are working in an enterprise. You project deals with important files that are stored on the computer. You have identified the risk of the failure of operations. To address this risk of failure, you have guided the system administrator sign off on the daily backup. This scenario is an example of which of the following?

A. Risk avoidance
B. Risk transference
C. Risk acceptance
D. Risk mitigation

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Here in this scenario, you are trying to reduce the risk of operation failure by guiding administrator to take daily backup, hence it is risk mitigation. Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together. The main control types are:
Managerial(e.g.,policies)
Technical (e.g., tools such as firewalls and intrusion detection systems) Operational (e.g., procedures, separation of duties) Preparedness activities
Answer: B is incorrect. The scenario does not describe the sharing of risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Answer: A is incorrect. The scenario does not describe risk avoidance. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk.
Answer: C is incorrect. The scenario does not describe risk acceptance, Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

QUESTION 106
Risks to an organization's image are referred to as what kind of risk?

A. Operational
B. Financial
C. Information
D. Strategic

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:

Explanation:
Strategic risks are those risks which have potential outcome of not fulfilling on strategic objectives of the organization as planned. Since the strategic objective will shape and impact the entire organization, the risk of not meeting that objective can impose a great threat on the organization.
Strategic risks can be broken down into external and internal risks:
External risks are those circumstances from outside the enterprise which will have a potentially damaging or helpful impact on the enterprise. These risks include sudden change of economy, industry, or regulatory conditions. Some of the external risks are predictable while others are not. For instance, a recession may be predictable and the enterprise may be able to hedge against the dangers economically; but the total market failure may not as predictable and can be much more devastating.
Internal risks usually focus on the image or reputation of the enterprise. some of the risks that are involved in this are public communication, trust, and strategic agreement from stakeholders and customers.
Reference: CRISC, Contents: "Assessing Risks"
Answer: B is incorrect. Financial risks are not directly linked with organization's reputation. Answer: C is incorrect. Risk associated with leakage of information to an unauthorized person does not affect organization's image.
Answer: A is incorrect. Operational risks are those risk that are associated with the day-to- day operations of the enterprise. They are generally more detailed as compared to strategic risks. It is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Some sub-categories of operational risks include:
Organizational or management related risks
Information security risks
Production, process, and productivity risks
Profitability operational risks
Business interruption risks
Project activity risks
Contract and product liability riss
Incidents and crisis
Illegal or malicious acts

QUESTION 107
Which of the following steps ensure effective communication of the risk analysis results to relevant stakeholders? Each correct answer represents a complete solution. Choose three.

A. The results should be reported in terms and formats that are useful to support business decisions
B. Provide decision makers with an understanding of worst-case and most probable scenarios, due diligence exposures and significant reputation, legal or regulatory considerations
C. Communicate the negative impacts of the events only, it needs more consideration
D. Communicate the risk-return context clearly

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:

Explanation:
The result of risk analysis process is being communicated to relevant stakeholders. The steps that are involved in communication are:
The results should be reported in terms and formats that are useful to support business decisions.
Coordinate additional risk analysis activity as required by decision makers, like report rejection and scope adjustment
Communicate the risk-return context clearly, which include probabilities of loss and/or gain, ranges, and confidence levels (if possible) that enable management to balance risk-return. Identify the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process.
Provide decision makers with an understanding of worst-case and most probable scenarios, due diligence exposures and significant reputation, legal or regulatory considerations. Answer: C is incorrect. Communicate the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process, for effective communication.
Only negative impacts are not considered alone.

QUESTION 108
You are the product manager in your enterprise. You have identified that new technologies, products and services are introduced in your enterprise time-to-time. What should be done to prevent the efficiency and effectiveness of controls due to these changes?

A. Receive timely feedback from risk assessments and through key risk indicators, and update controls
B. Add more controls
C. Perform Business Impact Analysis (BIA)
D. Nothing, efficiency and effectiveness of controls are not affected by these changes

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
As new technologies, products and services are introduced, compliance requirements become more complex and strict; business processes and related information flows change over time. These changes can often affect the efficiency and effectiveness of controls. Formerly effective controls become inefficient, redundant or obsolete and have to be removed or replaced.
Therefore, the monitoring process has to receive timely feedback from risk assessments and through key risk indicators (KRIs) to ensure an effective control life cycle. Answer: D is incorrect. Efficiency and effectiveness of controls are not affected by the changes in technology or product, so some measure should be taken. Answer: B is incorrect. Most of the time, the addition of controls results in degradation of the efficiency and profitability of a process without adding an equitable level of corresponding risk mitigation, hence better controls are adopted in place of adding more controls. Answer: C is incorrect. A BIA is a discovery process meant to uncover the inner workings of any process. It helps to identify about actual procedures, shortcuts, workarounds and the types of failure that may occur. It involves determining the purpose of the process, who performs the process and its output. It also involves determining the value of the process output to the enterprise.

QUESTION 109
Which of the following are sub-categories of threat? Each correct answer represents a complete solution. Choose three.

A. Natural and supernatural
B. Computer and user
C. Natural and man-made
D. Intentional and accidental
E. External and internal

Correct Answer: CDE
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
A threat is any event which have the potential to cause a loss. In other word, it is any activity that represents a possible danger. The loss or danger is directly related to one of the following:
Loss of confidentiality- Someone sees a password or a company's secret formula, this is referred to as loss of confidentiality. Loss of integrity- An e-mail message is modified in transit, a virus infects a file, or someone makes unauthorized changes to a Web site is referred to as loss of integrity.
Loss of availability- An e-mail server is down and no one has e-mail access, or a file server is down so data files aren't available comes under loss of availability.
Threat identification is the process of creating a list of threats. This list attempts to identify all the possible threats to an organization. The list can be extensive.
Threats are often sub-categorized as under:
External or internal- External threats are outside the boundary of the organization. They can also be thought of as risks that are outside the control of the organization. While internal threats are within the boundary of the organization. They could be related to employees or other personnel who have access to company resources. Internal threats can be related to any hardware or software controlled by the business.
Natural or man-made- Natural threats are often related to weather such as hurricanes, tornadoes, and ice storms. Natural disasters like earthquakes and tsunamis are also natural threats. A human or man-made threat is any threat which is caused by a person. Any attempt to harm resources is a man-made threat. Fire could be man-made or natural depending on how the fire is started. Intentional or accidental- An attempt to compromise confidentiality, integrity, or availability is intentional. While employee mistakes or user errors are accidental threats. A faulty application that corrupts data could also be considered accidental.

QUESTION 110
You work as a project manager for BlueWell Inc. Your project is using a new material to construct a large warehouse in your city. This new material is cheaper than traditional building materials, but it takes some time to learn how to use the material properly. You have communicated to the project stakeholders that you will be able to save costs by using the new material, but you will need a few extra weeks to complete training to use the materials. This risk response of learning how to use the new materials can also be known as what term?

A. Benchmarking
B. Cost-benefits analysis
C. Cost of conformance to quality
D. Team development

Correct Answer: C
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
When the project team needs training to be able to complete the project work it is a cost of conformance to quality.
The cost of conformance to quality defines the cost of training, proper resources, and the costs the project must spend in order to ascertain the expected levels of quality the customer expects from the project. It is the capital used up throughout the project to avoid failures. It consists of two types of costs:
Prevention costs: It is measured to build a quality product. It includes costs in training, document processing, equipment , and time to do it right. Appraisal costs: It is measured to assess the quality. It includes testing, destructive testing loss, and inspections.
Answer: D is incorrect. Team development describes activities the project manager uses to create a more cohesive and responsive project team. Answer: B is incorrect. Cost-benefit analysis is the study of the benefits in relation to the costs to receive the benefits of a decision, a project, or other investment. Answer: A is incorrect. Benchmarking compares any two items, such as materials, vendors, or resources.

QUESTION 111
What is the PRIMARY objective difference between an internal and an external risk management assessment reviewer?

A. In quality of work
B. In ease of access
C. In profession
D. In independence

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Independence is the freedom from conflict of interest and undue influence. By the mere fact that the external auditors belong to a different entity, their independence level is higher than that of the reviewer inside the entity for which they are performing a review. Independence is directly linked to objectivity.
Answer: C, A, and B are incorrect. These all choices vary subjectively.

QUESTION 112
You work as a Project Manager for www.company.com Inc. You have to measure the probability, impact, and risk exposure. Then, you have to measure how the selected risk response can affect the probability and impact of the selected risk event. Which of the following tools will help you to accomplish the task?

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

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
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 oppourtunities 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. Answer: D is incorrect. Cause-and-effect diagrams are useful for identifying root causes and risk identification, but they are not the most effective ones for risk response planning. Answer: A is incorrect. 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.
Answer: B is incorrect. The Delphi technique can be used in risk identification, but generally is not used in risk response planning. The Delphi technique uses rounds of anonymous surveys to identify risks.

QUESTION 113
Which of the following process ensures that extracted data are ready for analysis?

A. Data analysis
B. Data validation
C. Data gathering
D. Data access

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Data validation ensures that extracted data are ready for analysis. One objective is to perform data quality tests to ensure data are valid complete and free of errors. This may also involve making data from different sources suitable for comparative analysis. Answer: C is incorrect. Data gathering is the process of collecting data on risk to be monitored, prepare a detailed plan and define the project's scope. In the case of a monitoring project, this step should involve process owners, data owners, system custodians and other process stakeholders.
Answer: D is incorrect. In the data access process, management identifies which data are available and how they can be acquired in a format that can be used for analysis. There are two options for data extraction:
Extracting data directly from the source systems after system owner approval Receiving data extracts from the system custodian (IT) after system owner approval
Answer: A is incorrect. Analysis of data involves simple set of steps or complex combination of commands and other functionality. Data analysis is designed in such a way to achieve the stated objectives from the project plan. Although this may be applicable to any monitoring activity, it would be beneficial to consider transferability and scalability. This may include robust documentation, use of software development standards and naming conventions.

QUESTION 114
Which of the following vulnerability assessment software can check for weak passwords on the network?

A. Password cracker
B. Antivirus software
C. Anti-spyware software
D. Wireshark

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
A password cracker is an application program that is used to identify an unknown or forgotten password on a computer or network resources. It can also be used to help a human cracker obtain unauthorized access to resources. A password cracker can also check for weak passwords on the network and give notifications to put another password. Answer: B is incorrect. Antivirus or anti-virus software is used to prevent, detect, and remove malware. It scans the computer for viruses. Answer: C is incorrect. Anti-spyware software is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed. Answer: D is incorrect. Wireshark is a free and open-source protocol analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

QUESTION 115
Which of the following is NOT true for risk governance?

A. Risk governance is based on the principles of cooperation, participation, mitigation and sustainability, and is adopted to achieve more effective risk management.
B. Risk governance requires reporting once a year.
C. Risk governance seeks to reduce risk exposure and vulnerability by filling gaps in risk policy.
D. Risk governance is a systemic approach to decision making processes associated to natural and technological risks.

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Risk governance is a continuous life cycle that requires regular reporting and ongoing review, not once a year.
Answer: D, A, and C are incorrect. These are true for risk governace.

QUESTION 116

You are the project manager of HGT project. You have identified project risks and applied appropriate response for its mitigation. You noticed a risk generated as a result of applying response. What this resulting risk is known as?

A. Pure risk
B. Secondary risk
C. Response risk
D. High risk

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Secondary risk is a risk that is generated as the result of risk response. Answer: A is incorrect. A pure risk is a risk that has only a negative effect on the project. Pure risks are activities that are dangerous to complete and manage such as construction, electrical work, or manufacturing.
Answer: C and D are incorrect. These terms are not applied for the risk that is generated as a result of risk response.

QUESTION 117
What are the various outputs of risk response?

A. Risk Priority Number
B. Residual risk
C. Risk register updates
D. Project management plan and Project document updates
E. Risk-related contract decisions

Correct Answer: CDE
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The outputs of the risk response planning process are:
Risk Register Updates: The risk register is written in detail so that it can be related to the priority ranking and the planned response.
Risk Related Contract Decisions: Risk related contract decisions are the decisions to transmit risk, such as services, agreements for insurance, and other items as required. It provides a means for sharing risks.
Project Management Plan Updates: Some of the elements of the project management plan updates are:
Schedule management plan

Cost management plan
Quality management plan
Procurement management plan
Human resource management plan
Work breakdown structure
Schedule baseline
Cost performance baseline
Project Document Updates: Some of the project documents that can be updated includes:
Assumption log updates
Technical documentation updates
Answer: B is incorrect. Residual risk is not an output of risk response. Residual risk is the risk that remains after applying controls. It is not feasible to eliminate all risks from an organization. Instead, measures can be taken to reduce risk to an acceptable level. The risk that is left is residual risk.
As,
Risk = Threat Vulnerability and
Total risk = Threat Vulnerability Asset Value
Residual risk can be calculated with the following formula:
Residual Risk = Total Risk - Controls
Senior management is responsible for any losses due to residual risk. They decide whether a risk should be avoided, transferred, mitigated or accepted. They also decide what controls to implement. Any loss due to their decisions falls on their sides. Residual risk assessments are conducted after mitigation to determine the impact of the risk on the enterprise. For risk assessment, the effect and frequency is reassessed and the impact is recalculated.
Answer: A is incorrect. Risk priority number is not an output for risk response but instead it is done before applying response. Hence it act as one of the inputs of risk response and is not the output of it.

QUESTION 118
Which of the following is an output of risk assessment process?

A. Identification of risk
B. Identification of appropriate controls
C. Mitigated risk
D. Enterprise left with residual risk

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The output of the risk assessment process is identification of appropriate controls for reducing or eliminating risk during the risk mitigation process. To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Once risk factors have been identified, existing or new controls are designed and measured for their strength and likelihood of effectiveness. Controls are preventive, detective or corrective; manual or programmed; and formal or ad hoc. Answer: A is incorrect. Risk identification acts as input of the risk assessment

process. Answer: D is incorrect. Residual risk is the latter output after appropriate control. Answer: C is incorrect. This is an output of risk mitigation process, that is, after applying several risk responses.

QUESTION 119
What is the IMMEDIATE step after defining set of risk scenarios?

A. Risk mitigation
B. Risk monitoring
C. Risk management
D. Risk analysis

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Once the set of risk scenarios is defined, it can be used for risk analysis. In risk analysis, likelihood and impact of the scenarios are assessed. Important components of this assessment are the risk factors.
Answer: C is incorrect. Risk analysis comes under risk management, therefore management is a generalized term, and is not the best answer for this B is incorrect. Risk monitoring is the latter step after risk analysis and risk mitigation. Answer: A is incorrect. Risk mitigation is the latter step after analyzing risk.

QUESTION 120
Which of the following statements are true for risk communication? Each correct answer represents a complete solution. Choose three.

A. It requires a practical and deliberate scheduling approach to identify stakeholders, actions, and concerns.
B. It helps in allocating the information concerning risk among the decision-makers.
C. It requires investigation and interconnectivity of procedural, legal, social, political, and economic factors.
D. It defines the issue of what a stakeholders does, not just what it says.

Correct Answer: ACD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Risk communication is the process of exchanging information and views about risks among stakeholders, such as groups, individuals, and institutions. Risk communication is mostly concerned with the nature of risk or expressing concerns, views, or reactions to risk managers or institutional bodies for risk management. The key plan to consider and communicate risk is to categorize and impose priorities, and acquire suitable measures to reduce risks. It is important throughout any crisis to put across multifaceted information in a simple and clear manner.

Risk communication helps in switching or allocating the information concerning risk among the decision-maker and the stakeholders.
Risk communication can be explained more clearly with the help of the following definitions:
It defines the issue of what a group does, not just what it says. It must take into account the valuable element in user's perceptions of risk. It will be more valuable if it is thought of as conversation, not instruction. Risk communication is a fundamental and continuing element of the risk analysis exercise, and the involvement of the stakeholder group is from the beginning. It makes the stakeholders conscious of the process at each phase of the risk assessment. It helps to guarantee that the restrictions, outcomes, consequence, logic, and risk assessment are undoubtedly understood by all the stakeholders.
Answer: B is incorrect. It helps in allocating the information concerning risk not only among the decision-makers but also stakeholders.

QUESTION 121
Which of the following is the most accurate definition of a project risk?

A. It is an unknown event that can affect the project scope.
B. It is an uncertain event or condition within the project execution.
C. It is an uncertain event that can affect the project costs.
D. It is an uncertain event that can affect at least one project objective.

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Risk is an uncertain event or condition that, if it occurs, has an effect on at least one project objective.
Project risk is concerned with the expected value of one or more results of one or more future events in a project. It is an uncertain condition that, if it occurs, has an effect on at least one project objective. Objectives can be scope, schedule, cost, and quality. Project risk is always in the future.
Answer: A is incorrect. Risk is not unknown, it is uncertain; in addition, the event can affect at least one project objective - not just the project scope. Answer: B is incorrect. This statement is almost true, but the event does not have to happen within project execution.
Answer: C is incorrect. Risks can affect time, costs, or scope, rather affecting only cost.

QUESTION 122
Which of the following considerations should be taken into account while selecting risk indicators that ensures greater buy-in and ownership?

A. Lag indicator
B. Lead indicator
C. Root cause
D. Stakeholder

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
To ensure greater buy-in and ownership, risk indicators should be selected with the involvement of relevant stakeholders. Risk indicators should be identified for all stakeholders and should not focus solely on the more operational or strategic side of risk. Answer: B is incorrect. Lead indicators indicate which capabilities are in place to prevent events from occurring. They do not play any role in ensuring greater buy-in and ownership. Answer: A is incorrect. Role of lag indicators is to ensure that risk after events have occurred is being indicated.
Answer: C is incorrect. Root cause is considered while selecting risk indicator but it does not ensure greater buy-in or ownership.

QUESTION 123
Suppose you are working in Techmart Inc. which sells various products through its website. Due to some recent losses, you are trying to identify the most important risks to the Website. Based on feedback from several experts, you have come up with a list. You now want to prioritize these risks. Now in which category you would put the risk concerning the modification of the Website by unauthorized parties.

A. Ping Flooding Attack
B. Web defacing
C. Denial of service attack
D. FTP Bounce Attack

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Website defacing is an attack on a website by unauthorized party that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own. Answer: D is incorrect. The FTP bounce attack is attack which slips past application-based firewalls. In this hacker uploads a file to the FTP server and then requests this file be sent to an internal server. This file may contain malicious software or a simple script that occupies the internal server and uses up all the memory and CPU resources. Answer: A is incorrect. Ping Flooding is the extreme of sending thousands or millions of pings per second. Ping Flooding attack can make system slow or even shut down an entire site.
Answer: C is incorrect. A denial-of-service attack (DoS attack) is an attempt to make a computer or network resource unavailable to its intended users. One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

QUESTION 124
Which of the following is true for risk evaluation?

A. Risk evaluation is done only when there is significant change.
B. Risk evaluation is done once a year for every business processes.
C. Risk evaluation is done annually or when there is significant change.

D. Risk evaluation is done every four to six months for critical business processes.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Due to the reason that risk is constantly changing, it is being evaluated annually or when there is significant change. This gives best alternative as it takes into consideration a reasonable time frame of one year, and meanwhile it also addresses significant changes (if any).
Answer: A is incorrect. Evaluating risk only when there is significant changes do not take into consideration the effect of time. As the risk is changing constantly, small changes do occur with time that would affect the overall risk. Hence risk evaluation should be done annually too.
Answer: D is incorrect. Risk evaluation need not to be done every four to six months for critical processes, as it does not addresses important changes in timely manner. Answer: B is incorrect. Evaluating risk once a year is not sufficient in the case when some significant change takes place. This significant change should be taken into account as it affects the overall risk.

QUESTION 125
You work as a project manager for Bluewell Inc. You have identified a project risk. You have then implemented the risk action plan and it turn out to be non-effective. What type of plan you should implement in such case?

A. Risk mitigation
B. Risk fallback plan
C. Risk avoidance
D. Risk response plan

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
A risk fallback plan is a proper plan devised to identify definite action to be taken if the risk action plan (Risk Mitigation Plan) is not helpful. Fallback plan is important in Risk Response Planning. If the contingency plan for a risk is not successful, then the project team implements the fallback plan. Fall-back planning is intended for a known and specific activity that may perhaps fail to produce desired outcome. It is related with technical procedures and with the responsibility of the technical lead.
Answer: D, A, and C are incorrect. These all choices itself comes under risk action plan. As in the described scenario, risk action plan is not turned to be effective, these should not be implemented again.

QUESTION 126
You are completing the qualitative risk analysis process with your project team and are relying on the risk management plan to help you determine the budget, schedule for risk management, and risk categories. You discover that the risk categories have not been created.

When the risk categories should have been created?

A. Define scope process
B. Risk identification process
C. Plan risk management process
D. Create work breakdown structure process

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The plan risk management process is when risk categories were to be defined. If they were not defined, as in this scenario, it is acceptable to define the categories as part of the qualitative risk analysis process.
Plan risk management is the process of defining the way to conduct the risk management activities. Planning is essential for providing sufficient resources and time for risk management activities, and to establish a agreed-upon basis of evaluating risks. This process should start as soon as project is conceived and should be completed early during project planning.
Answer: A is incorrect. Risk categories are not defined through the define scope process. Answer: D is incorrect. Risk categories are not defined through the create work breakdown structure process.
Answer: B is incorrect. Risk categories are not defined through the risk identification process.

QUESTION 127
You work as a project manager for BlueWell Inc. You have declined a proposed change request because of the risk associated with the proposed change request. Where should the declined change request be documented and stored?

A. Change request log
B. Project archives
C. Lessons learned
D. Project document updates

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The change request log records the status of all change requests, approved or declined. The change request log is used as an account for change requests and as a means of tracking their disposition on a current basis. The change request log develops a measure of consistency into the change management process. It encourages common inputs into the process and is a common estimation approach for all change requests. As the log is an important component of project

requirements, it should be readily available to the project team members responsible for project delivery. It should be maintained in a file with read- only access to those who are not responsible for approving or disapproving project change requests.
Answer: C is incorrect. Lessons learned are not the correct place to document the status of a declined, or approved, change request.
Answer: B is incorrect. The project archive includes all project documentation and is created through the close project or phase process. It is not the best choice for this option D is incorrect. The project document updates is not the best choice for this QUESTION NO: be placed into the project documents, but the declined changes are part of the change request log.

QUESTION 128
Capability maturity models are the models that are used by the enterprise to rate itself in terms of the least mature level to the most mature level. Which of the following capability maturity levels shows that the enterprise does not recognize the need to consider the risk management or the business impact from IT risk?

A. Level 2
B. Level 0
C. Level 3
D. Level 1

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
0 nonexistent: An enterprise's risk management capability maturity level is 0 when:
The enterprise does not recognize the need to consider the risk management or the business impact from IT risk.
Decisions involving risk lack credible information. Awareness of external requirements for risk management and integration with enterprise risk management (ERM) do not exists.
Answer: D, A, and C are incorrect. These all are higher levels of capability maturity model and in this enterprise is mature enough to recognize the importance of risk management.

QUESTION 129
Using which of the following one can produce comprehensive result while performing qualitative risk analysis?

A. Scenarios with threats and impacts
B. Cost-benefit analysis
C. Value of information assets.
D. Vulnerability assessment

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Using list of possible scenarios with threats and impacts will better frame the range of risk and hence can frame more informative result of qualitative analysis. Answer: B is incorrect. Cost and benefit analysis is used for taking financial decisions that can be formal or informal, such as appraisal of any project or proposal. The approach weighs the total cost against the benefits expected, and then identifies the most profitable option. It only decides what type of control should be applied for effective risk management. Answer: D and C are incorrect. These are not sufficient for producing detailed result.

QUESTION 130
Which of the following is the BEST method for discovering high-impact risk types?

A. Qualitative risk analysis
B. Delphi technique
C. Failure modes and effects analysis
D. Quantitative risk analysis

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Failure modes and effects analysis is used in discovering high-impact risk types.
FMEA:
Is one of the tools used within the Six Sigma methodology to design and implement a robust process to:
Identify failure modes
Establish a risk priority so that corrective actions can be put in place to address and reduce the risk
Helps in identifying and documenting where in the process the source of the failure impacts the (internal or external) customer
Is used to determine failure modes and assess risk posed by the process and thus, to the enterprise as a whole'
Answer: D and A are incorrect. These two are the methods of analyzing risk, but not specifically for high-impact risk types. Hence is not the best answer. Answer: B is incorrect. Delphi is a technique to identify potential risk. In this technique, the responses are gathered via a question: and their inputs are organized according to their contents. The collected responses are sent back to these experts for further input, addition, and comments. The final list of risks in the project is prepared after that. The participants in this technique are anonymous and therefore it helps prevent a person from unduly influencing the others in the group. The Delphi technique helps in reaching the consensus quickly.

QUESTION 131
Which of the following is MOST appropriate method to evaluate the potential impact of legal, regulatory, and contractual requirements on business objectives?

A. Communication with business process stakeholders
B. Compliance-oriented business impact analysis

C. Compliance-oriented gap analysis
D. Mapping of compliance requirements to policies and procedures

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
A compliance-oriented BIA will identify all the compliance requirements to which the enterprise has to align and their impacts on business objectives and activities. It is a discovery process meant to uncover the inner workings of any process. Hence it will also evaluate the potential impact of legal, regulatory, and contractual requirements on business objectives. Answer: D is incorrect. Mapping of compliance requirements to policies and procedures will identify only the way the compliance is achieved but not the business impact. Answer: A is incorrect. Communication with business process stakeholders is done so as to identify the business objectives, but it does not help in identifying impacts. Answer: C is incorrect. Compliance-oriented gap analysis will only identify the gaps in compliance to current requirements and will not identify impacts to business objectives.

QUESTION 132
Wendy is about to perform qualitative risk analysis on the identified risks within her project. Which one of the following will NOT help Wendy to perform this project management activity?

A. Risk management plan
B. Project scope statement
C. Risk register
D. Stakeholder register

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The stakeholder register is not an input to the qualitative risk analysis process. The four inputs are the risk register, risk management plan, project scope statement, and organizational process assets.
Answer: C is incorrect. The risk register can help Wendy to perform qualitative risk analysis. Answer: B is incorrect. The project scope statement is needed to help with qualitative risk analysis.
Answer: A is incorrect. The Risk management plan is an input to the risk qualitative analysis process.

QUESTION 133
There are four inputs to the Monitoring and Controlling Project Risks process. Which one of the following will NOT help you, the project manager, to prepare for risk monitoring and controlling?

A. Risk register
B. Work Performance Information
C. Project management plan
D. Change requests

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Change requests are not one of the four inputs to the Risk Monitoring and Controlling Process. The four inputs are the risk register, the project management plan, work performance information, and performance reports.
Answer: A, C, and B are incorrect. These are the valid inputs to the Risk Monitoring and Controlling Process.

QUESTION 134
You are the project manager of HWD project. It requires installation of some electrical machines. You and the project team decided to hire an electrician as electrical work can be too dangerous to perform. What type of risk response are you following?

A. Avoidance
B. Transference
C. Mitigation
D. Acceptance

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
As the risk is transferred to the third party (electrician), hence this type of risk response is transference.
Answer: A is incorrect. Risk avoidance means to evade risk altogether, eliminate the cause of the risk event, or change the project plan to protect the project objectives from the risk event. Risk avoidance is applied when the level of risk, even after the applying controls, would be greater than the risk tolerance level of the enterprise. Answer: D is incorrect. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs.
Answer: C is incorrect. Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together.

QUESTION 135
You are the project manager of GHT project. You have implemented an automated tool to analyze and report on access control logs based on severity. This tool

generates excessively large amounts of results. You perform a risk assessment and decide to configure the monitoring tool to report only when the alerts are marked "critical". What you should do in order to fulfill that?

A. Apply risk response
B. Optimize Key Risk Indicator
C. Update risk register
D. Perform quantitative risk analysis

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
As the sensitivity of the monitoring tool has to be changed, therefore it requires optimization of Key Risk Indicator. The monitoring tool which is giving alerts is itself acting as a risk indicator. Hence to change the sensitivity of the monitoring tool to give alert only for critical situations requires optimization of the KRI.
Answer: A, C, and D are incorrect. These options are not relevant to the change of sensitivity of the monitoring tools.

QUESTION 136
One of the risk events you've identified is classified as force majeure. What risk response is likely to be used?

A. Acceptance
B. Transference
C. Enhance
D. Mitigation

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Force majeure describes acts of God (Natural disaster), such as tornados and fires, and are usually accepted because there's little than can be done to mitigate these risks. Answer: D is incorrect. Mitigation isn't the best choice, as this lowers the probability and/or impact of the risk event.
Answer: C is incorrect. Enhance is used for a positive risk event, not for force majeure. Answer: B is incorrect. Transference transfers the risk ownership to a third party, usually for a fee.

QUESTION 137
You are the project manager of GHT project. You have applied certain control to prevent the unauthorized changes in your project. Which of the following control you would have applied for this purpose?

A. Personnel security control
B. Access control
C. Configuration management control
D. Physical and environment protection control

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Configuration management control is a family of controls that addresses both configuration management and change management. Change control practices prevent unauthorized changes. They include goals such as configuring systems for least functionality as a primary method of hardening systems.
Answer: D is incorrect. Physical and environment protection control are the family that provides an extensive number of controls related to physical security.
Answer: A is incorrect. The Personal security control is family of controls that includes aspects of personnel security. It includes personnel screening, termination, and transfer. Answer: B is incorrect. 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.

QUESTION 138
You are the project manager for BlueWell Inc. You have noticed that the risk level in your project increases above the risk tolerance level of your enterprise. You have applied several risk response. Now you have to update the risk register in accordance to risk response process. All of the following are included in the risk register except for which item?

A. Risk triggers
B. Agreed-upon response strategies
C. Network diagram analysis of critical path activities
D. Risk owners and their responsibility

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The risk register does not examine the network diagram and the critical path. There may be risks associated with the activities on the network diagram, but it does not address the network diagram directly.
The risk register is updated at the end of the plan risk response process with the information that was discovered during the process. The response plans are recorded in the risk register. In the risk register, risk is stated in order of priority, i.e., those with the highest potential for threat or opportunity first. Some risks might not require response plans at all, but then too they should be put on a watch list and monitored throughout the project. Following elements should appear in the risk

register:
List of identified risks, including their descriptions, root causes, and how the risks impact the project objectives
Risk owners and their responsibility
Outputs from the Perform Qualitative Analysis process Agreed-upon response strategies
Risk triggers
Cost and schedule activities needed to implement risk responses Contingency plans
Fallback plans, which are risk response plans that are executed when the initial risk response plan proves to be ineffective
Contingency reserves
Residual risk, which is a leftover risk that remains after the risk response strategy has been implemented Secondary risks, which are risks that come about as a result of implementing a risk response

QUESTION 139
Ben is the project manager of the CMH Project for his organization. He has identified a risk that has a low probability of happening, but the impact of the risk event could save the project and the organization with a significant amount of capital. Ben assigns Laura to the risk event and instructs her to research the time, cost, and method to improve the probability of the positive risk event. Ben then communicates the risk event and response to management. What risk response has been used here?

A. Transference
B. Enhance
C. Exploit
D. Sharing

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Enhance is a risk response to improve the conditions to ensure the risk event occurs. Risk enhancement raises the probability of an opportunity to take place by focusing on the trigger conditions of the opportunity and optimizing the chances. Identifying and maximizing input drivers of these positive-impact risks may raise the probability of their occurrence. Answer: A is incorrect. Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference. Answer: C is incorrect. 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: D is incorrect. Sharing happens through partnerships, joint ventures, and teaming agreements. Sharing response is where two or more entities share a positive risk. Teaming agreements are good example of sharing the reward that comes from the risk of the opportunity.

QUESTION 140
Which of the following techniques examines the degree to which organizational strengths offset threats and opportunities that may serve to overcome weaknesses?

A. SWOT Analysis
B. Delphi
C. Brainstorming
D. Expert Judgment

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
SWOT analysis is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats involved in a project or in a business venture. It involves specifying the objective of the business venture or project and identifying the internal and external factors that are favorable and unfavorable to achieving that objective. Answer: C and B are incorrect. Brainstorming and Delphi techniques are used to identify risks in a project through consensus. Delphi differs in that as the members of the team do not know each other.
Answer: D is incorrect. In this technique, risks can be identified directly by experts with relevant experience of similar projects or business areas.

QUESTION 141
You are the project manager for your company and a new change request has been approved for your project. This change request, however, has introduced several new risks to the project. You have communicated these risk events and the project stakeholders understand the possible effects these risks could have on your project. You elect to create a mitigation response for the identified risk events. Where will you record the mitigation response?

A. Risk register
B. Risk log
C. Project management plan
D. Risk management plan

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The Identified risks and potential responses are documented in the risk register. A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains:
A description of the risk
The impact should this event actually occur
The probability of its occurrence
Risk Score (the multiplication of Probability and Impact) A summary of the planned response should the event occur A summary of the mitigation (the actions taken

in advance to reduce the probability and/or impact of the event)
Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved. Answer: D is incorrect. The risk management plan is an input to the risk response planning, but it is not the best choice for this question option B is incorrect. This is not a valid choice for the question option C is incorrect. The project management plan is the parent of the risk management plan, but the best choice is the risk register.

QUESTION 142
Which of the following actions assures management that the organization's objectives are protected from the occurrence of risk events?

A. Internal control
B. Risk management
C. Hedging
D. Risk assessment

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Internal controls are the actions taken by the organization to help to assure management that the organization's objectives are protected from the occurrence of risk events. Internal control objectives are applicable to all manual or automated areas. Internal control objectives include:
Internal accounting controls- They control accounting operations, including safeguarding assets and financial records.
Operational controls- They focus on day-to-day operations, functions, and activities. They ensure that all the organization's objectives are being accomplished.
Administrative controls- They focus on operational efficiency in a functional area and stick to management policies.
Answer: D is incorrect. 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.
Answer: B is incorrect. Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources. It is done to minimize, monitor, and control the probability and impact of unfortunate events or to maximize the realization of opportunities.
Answer: C is incorrect. Hedging is the process of managing the risk of price changes in physical material by offsetting that risk in the futures market. In other words, it is the avoidance of risk. So, it only avoids risk but can not assure protection against risk.

QUESTION 143
You are working as a project manager in Bluewell Inc.. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

A. Qualitative risk analysis

B. Risk audits

C. Quantitative risk analysis

D. Requested changes

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Of all the choices given, only requested changes is an output of the monitor and control risks process. You might also have risk register updates, recommended corrective and preventive actions, organizational process assets, and updates to the project management plan. Answer: A and C are incorrect. These are the plan risk management processes. Answer: B is incorrect. Risk audit is a risk monitoring and control technique.

QUESTION 144
You are the project manager of HGT project. You are in the first phase of the risk response process and are doing following tasks :
Communicating risk analysis results
Reporting risk management activities and the state of compliance Interpreting independent risk assessment findings
Identifying business opportunities
Which of the following process are you performing?

A. Articulating risk

B. Mitigating risk

C. Tracking risk

D. Reporting risk

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Articulating risk is the first phase in the risk response process to ensure that information on the true state of exposures and opportunities are made available in a timely manner and to the right people for appropriate response. Following are the tasks that are involved in articulating risk:
Communicate risk analysis results.
Report risk management activities and the state of compliance.
Interpret independent risk assessment findings.
Identify business opportunities.
Answer: B is incorrect. Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together. This comes under risk response process and is latter stage after articulating risk.

Answer: D is incorrect. This is not related to risk response process. It is a type of risk. Reporting risks are the risks that are caused due to wrong reporting which leads to bad decision.
Answer: C is incorrect. Tracking risk is the process of tracking the ongoing status of risk mitigation processes. This tracking ensures that the risk response strategy remains active and that proposed controls are implemented according to schedule.

QUESTION 145
Which of the following BEST measures the operational effectiveness of risk management capabilities?

A. Capability maturity models (CMMs)
B. Metric thresholds
C. Key risk indicators (KRIs)
D. Key performance indicators (KPIs)

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Key performance indicators (KPIs) provide insights into the operational effectiveness of the concept or capability that they monitor. Key Performance Indicators is a set of measures that a company or industry uses to measure and/or compare performance in terms of meeting their strategic and operational goals. KPIs vary with company to company, depending on their priorities or performance criteria.
A company must establish its strategic and operational goals and then choose their KPIs which can best reflect those goals. For example, if a software company's goal is to have the fastest growth in its industry, its main performance indicator may be the measure of its annual revenue growth.
Answer: C is incorrect. Key risk indicators (KRIs) only provide insights into potential risks that may exist or be realized within a concept or capability that they monitor. 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.
Answer: A is incorrect. Capability maturity models (CMMs) assess the maturity of a concept or capability and do not provide insights into operational effectiveness.
Answer: B is incorrect. Metric thresholds are decision or action points that are enacted when a KPI or KRI reports a specific value or set of values. It odes not provide any insights into operational effectiveness.

QUESTION 146
You are the project manager of GHT project. You have initiated the project and conducted the feasibility study. What result would you get after conducting feasibility study? Each correct answer represents a complete solution. Choose all that apply.

A. Recommend alternatives and course of action
B. Risk response plan
C. Project management plan
D. Results of criteria analyzed, like costs, benefits, risk, resources required and organizational impact

Correct Answer: AD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The completed feasibility study results should include a cost/benefit analysis report that:
Provides the results of criteria analyzed (e.g., costs, benefits, risk, resources required and organizational impact)
Recommends one of the alternatives and a course of action Answer: C and B are incorrect. Project management plan and risk response plan are the results of plan project management and plan risk response, respectively. They are not the result of feasibility study.

QUESTION 147
Your project change control board has approved several scope changes that will drastically alter your project plan. You and the project team set about updating the project scope, the WBS, the WBS dictionary, the activity list, and the project network diagram. There are also some changes caused to the project risks, communication, and vendors. What also should the project manager update based on these scope changes?

A. Stakeholder identification
B. Vendor selection process
C. Quality baseline
D. Process improvement plan

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
When changes enter the project scope, the quality baseline is also updated. The quality baseline records the quality objectives of the project and is based on the project requirements. Answer: D is incorrect. The process improvement plan aims to improve the project's processes regardless of scope changes.
Answer: B is incorrect. The vendor selection process likely will not change because of added scope changes. The vendors in the project may, but the selection process will not. Answer: A is incorrect. The stakeholder identification process will not change because of scope additions. The number of stakeholders may change but how they are identified will not be affected by the scope addition.

QUESTION 148
You are the risk control professional of your enterprise. You have implemented a tool that correlates information from multiple sources. To which of the following do this monitoring tool focuses?

A. Transaction data
B. Process integrity
C. Configuration settings

D. System changes

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Monitoring tools that focuses on transaction data generally correlate information from one system to another, such as employee data from the human resources (HR) system with spending information from the expense system or the payroll system. Answer: B is incorrect. Process integrity is confirmed within the system, it dose not need monitoring.
Answer: D is incorrect. System changes are compared from a previous state to the current state, it dose not correlate information from multiple sources. Answer: C is incorrect. Configuration settings are generally compared against predefined values and not based on the correlation between multiple souces.

QUESTION 149
Which of the following are the security plans adopted by the organization? Each correct answer represents a complete solution. Choose all that apply.

A. Business continuity plan
B. Backup plan
C. Disaster recovery plan
D. Project management plan

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Organizations create different security plans to address different scenarios. Many of the security plans are common to most organizations.
Most used security plans found in many organizations are:
Business continuity plan
Disaster recovery plan
Backup plan
Incident response plan
Answer: D is incorrect. Project management plan is not a security plan, but a plan which describes the implementation of the project.

QUESTION 150
Which of the following guidelines should be followed for effective risk management? Each correct answer represents a complete solution. Choose three.

A. Promote and support consistent performance in risk management

B. Promote fair and open communication
C. Focus on enterprise's objective
D. Balance the costs and benefits of managing risk

Correct Answer: BCD
Section: Volume B
Explanation

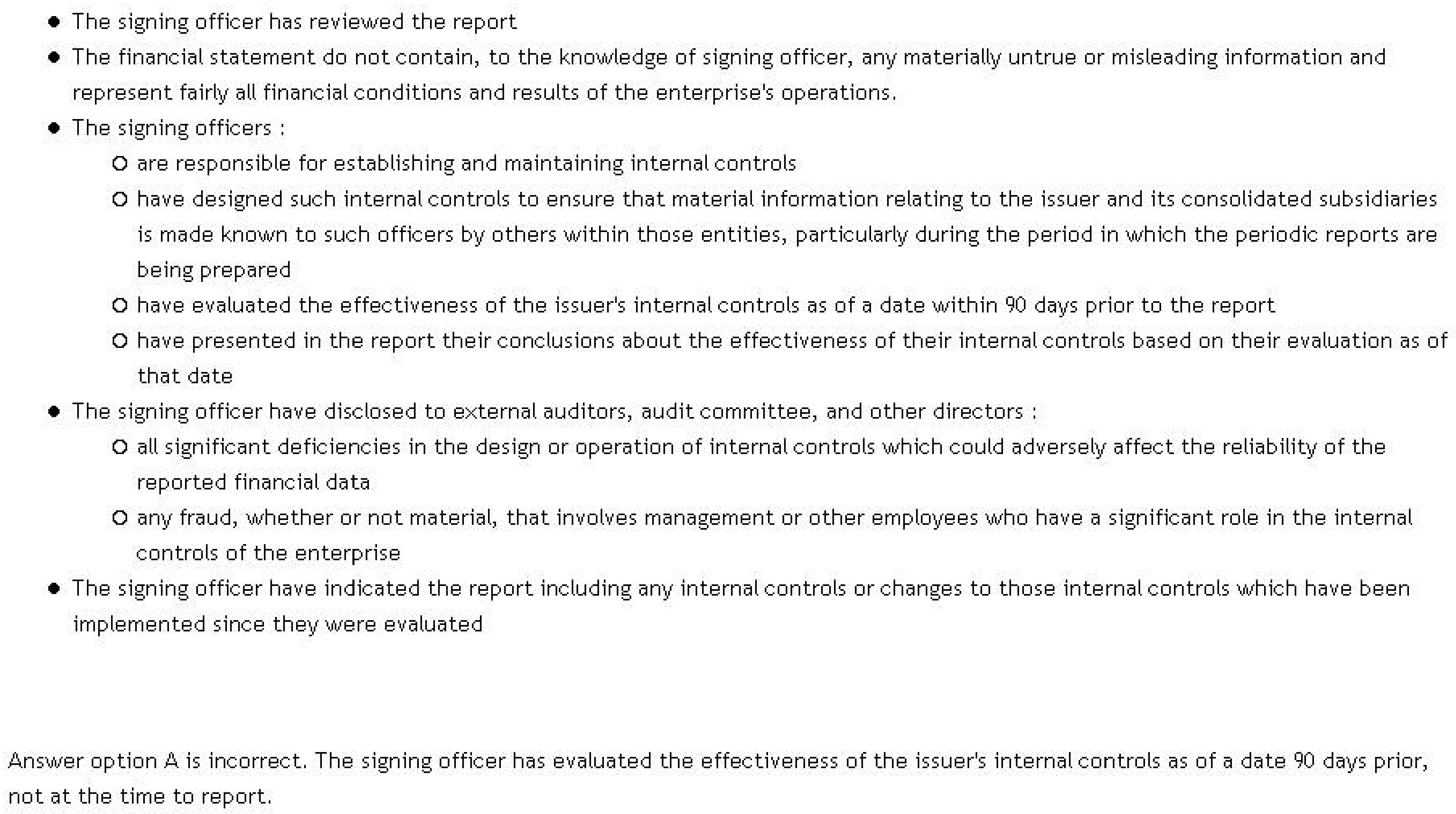
Explanation/Reference:
Explanation:
The primary function of the enterprise is to meet its objective. Each business activity for fulfilling enterprise's objective carries both risk and opportunity, therefore objective should be considered while managing risk.
Open and fair communication should me there for effective risk management. Open, accurate, timely and transparent information on lT risk is exchanged and serves as the basis for all risk-related decisions.
Cost-benefit analysis should be done for proper weighing the total costs expected against the total benefits expected, which is the major aspect of risk management. Answer: A is incorrect. For effective risk management, there should be continuous improvement, not consistent. Because of the dynamic nature of risk, risk management is an iterative, perpetual and ongoing process; that's why, continuous improvement is required.

QUESTION 151
According to the Section-302 of the Sarbanes-Oxley Act of 2002, what does certification of reports implies? Each correct answer represents a complete solution. Choose three.

A. The signing officer has evaluated the effectiveness of the issuer's internal controls as of a date at the time to report.
B. The financial statement does not contain any materially untrue or misleading information.
C. The signing officer has reviewed the report.
D. The signing officer has presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date.

Correct Answer: BCD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Section 302 of Sarbanes-Oxley act has the tremendous impact on the risk management solution adopted by corporations. This section specifies that the reports must be certified by the CEO, CFO, or other senior officer performing similar functions.
Certification of reports establishes:



- The signing officer has reviewed the report
- The financial statement do not contain, to the knowledge of signing officer, any materially untrue or misleading information and represent fairly all financial conditions and results of the enterprise's operations.
- The signing officers :
  - are responsible for establishing and maintaining internal controls
  - have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared
  - have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report
  - have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date
- The signing officer have disclosed to external auditors, audit committee, and other directors :
  - all significant deficiencies in the design or operation of internal controls which could adversely affect the reliability of the reported financial data
  - any fraud, whether or not material, that involves management or other employees who have a significant role in the internal controls of the enterprise
- The signing officer have indicated the report including any internal controls or changes to those internal controls which have been implemented since they were evaluated

Answer option A is incorrect. The signing officer has evaluated the effectiveness of the issuer's internal controls as of a date 90 days prior, not at the time to report.

QUESTION 152

Thomas is a key stakeholder in your project. Thomas has requested several changes to the project scope for the project you are managing.
Upon review of the proposed changes, you have discovered that these new requirements are laden with risks and you recommend to the change control board that the changes be excluded from the project scope. The change control board agrees with you. What component of the change control system communicates the approval or denial of a proposed change request?

A. Configuration management system
B. Integrated change control
C. Change log
D. Scope change control system

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Integrated change control is responsible for facilitating, documenting, and dispersing information on a proposed change to the project scope. Integrated change control is a way to manage the changes incurred during a project. It is a method that manages reviewing the suggestions for changes and utilizing the tools and techniques to evaluate whether the change should be approved or rejected. Integrated change control is a primary component of the project's change control system that examines the affect of a proposed change on the entire project.
Answer: D is incorrect. The scope change control system controls changes that are permitted to the project scope.
Answer: A is incorrect. The configuration management system controls and documents changes to the project's product
Answer: C is incorrect. The change log documents approved changes in the project scope.

QUESTION 153
Which of the following process ensures that the risk response strategy remains active and that proposed controls are implemented according to schedule?

A. Risk management
B. Risk response integration
C. Risk response implementation
D. Risk response tracking

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Risk response tracking tracks the ongoing status of risk mitigation processes as part of risk response process. This tracking ensures that the risk response strategy remains active and that proposed controls are implemented according to schedule. When an enterprise is conscious of a risk, but does not have an appropriate risk response strategy, then it lead to the increase of the liability of the organization to adverse publicity or even civil or criminal penalties. Answer: C is incorrect. Implementation of risk response ensures that the risks analyzed in risk analysis process are being lowered to level that the enterprise can accept, by applying appropriate controls.
Answer: B is incorrect. Integrating risk response options to address more than one risk together, help in achieving greater efficiency.
The use of techniques that are versatile and enterprise-wide, rather than individual solutions provides better justification for risk response strategies and related

costs. Answer: A is incorrect. Risk management provides an approach for individuals and groups to make a decision on how to deal with potentially harmful situations

QUESTION 154
Which of the following individuals is responsible for identifying process requirements, approving process design and managing process performance?

A. Business process owner
B. Risk owner
C. Chief financial officer
D. Chief information officer

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Business process owners are the individuals responsible for identifying process requirements, approving process design and managing process performance. In general, a business process owner must be at an appropriately high level in the enterprise and have authority to commit resources to process-specific risk management activities. Answer: B is incorrect. Risk owner for each risk should be the person who has the most influence over its outcome. Selecting the risk owner thus usually involves considering the source of risk and identifying the person who is best placed to understand and implement what needs to be done. Answer: C is incorrect. Chief financial officer is the most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks. Answer: D is incorrect. Chief information officer 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.

QUESTION 155
Which of the following should be considered to ensure that risk responses that are adopted are cost-effective and are aligned with business objectives? Each correct answer represents a part of the solution. Choose three.

A. Identify the risk in business terms
B. Recognize the business risk appetite
C. Adopt only pre-defined risk responses of business
D. Follow an integrated approach in business

Correct Answer: ABD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:

Risk responses require a formal approach to issues, opportunities and events to ensure that solutions are cost-effective and are aligned with business objectives. The following should be considered:
While preparing the risk response, identify the risk in business terms like loss of productivity, disclosure of confidential information, lost opportunity costs, etc.
Recognize the business risk appetite.
Follow an integrated approach in business.
Risk responses requiring an investment should be supported by a carefully planned business case that justifies the expenditure outlines alternatives and describes the justification for the alternative selected.
Answer: C is incorrect. There is no such requirement to follow the pre-defined risk responses. If some new risk responses are discovered during the risk management of a particular project, they should be noted down in lesson leaned document so that project manager working on some other project could also utilize them.

QUESTION 156
Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

A. Project management plan
B. Project communications plan
C. Project contractual relationship with the vendor
D. Project scope statement

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
When new risks are identified as part of the scope additions, Walter should update the risk register and the project management plan to reflect the responses to the risk event. Answer: D is incorrect. The project scope statement is changed as part of the scope approval that has already happened.
Answer: C is incorrect. The contractual relationship won't change with the vendor as far as project risks are concerned.
Answer: B is incorrect. The project communications management plan may be updated if there's a communication need but the related to the risk event, not the communication of the risks.

QUESTION 157
What are the three PRIMARY steps to be taken to initialize the project? Each correct answer represents a complete solution. Choose all that apply.

A. Conduct a feasibility study
B. Define requirements

C. Acquire software

D. Plan risk management

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Projects are initiated by sponsors who gather the information required to gain approval for the project to be created. Information often compiled into the terms of a project charter includes the objective of the project, business case and problem statement, stakeholders in the system to be produced, and project manager and sponsor.
Following are the steps to initiate the project:
Conduct a feasibility study: Feasibility study starts once initial approval has been given to move forward with a project, and includes an analysis to clearly define the need and to identify alternatives for addressing the need. A feasibility study involves:
Analyzing the benefits and solutions for the identified problem area Development of a business case that states the strategic benefits of implementing the system cither in productivity gains or in future cost avoidance and identifies and quantifies the cost savings of the new system.
Estimation of a payback schedule for the cost incurred in implementing the system or shows the projected return on investment (ROI)
Define requirements: Requirements include:
Business requirements containing descriptions of what a system should do Functional requirements and use case models describing how users will interact with a system
Technical requirements and design specifications and coding specifications describing how the system will interact, conditions under which the system will operate and the information criteria the system should meet.
Acquire software: Acquiring software involves building new or modifying existing hardware or software after final approval by the stakeholder, which is not a phase in the standard SDLC process. If a decision was reached to acquire rather than develop software, this task should occur after defining requirements.
Answer: D is incorrect. Risk management is planned latter in project development process, and not during initialization.

QUESTION 158
You are the risk official in Techmart Inc. You are asked to perform risk assessment on the impact of losing a network connectivity for 1 day. Which of the following factors would you include?

A. Aggregate compensation of all affected business users.

B. Hourly billing rate charged by the carrier

C. Value that enterprise get on transferring data over the network

D. Financial losses incurred by affected business units

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The impact of network unavailability is the cost it incurs to the enterprise. As the network is unavailable for 1 day, it can be considered as the failure of some business units that rely on this network. Hence financial losses incurred by this affected business unit should be considered.
Answer: B, C, and A are incorrect. These factors in combination contribute to the overall financial impact, i.e., financial losses incurred by affected business units.

QUESTION 159
Beth is a project team member on the JHG Project. Beth has added extra features to the project and this has introduced new risks to the project work. The project manager of the JHG project elects to remove the features Beth has added. The process of removing the extra features to remove the risks is called what?

A. Detective control
B. Preventive control
C. Corrective control
D. Scope creep

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
This is an example of a preventive control as the problem is not yet occurred, only it is detected and are accounted for. By removing the scope items from the project work, the project manager is aiming to remove the added risk events, hence it is a preventive control. Preventive control is a type of internal control that is used to avoid undesirable events, errors and other occurrences, which an organization has determined could have a negative material effect on a process or end product.
Answer: C is incorrect. Corrective actions are steps to bring the future performance of the project work in line with the project management plan. These controls make effort to reduce the impact of a threat from problems discovered by detective controls. They first identify the cause of the problems, then take corrective measures and modify the systems to minimize the future occurrences of the problem. Hence an incident should take place before corrective controls come in action.
Answer: A is incorrect. Detective controls simply detect and report on the occurrence of problems. They identify specific symptoms to potential problems. Answer: D is incorrect. Scope creep refers to small undocumented changes to the project scope.

QUESTION 160
You are the project manager of the GHT project. This project will last for 18 months and has a project budget of $567,000. Robert, one of your stakeholders, has introduced a scope change request that will likely have an impact on the project costs and schedule. Robert assures you that he will pay for the extra time and costs associated with the risk event. You have identified that change request may also affect other areas of the project other than just time and cost. What project management component is responsible for evaluating a change request and its impact on all of the project management knowledge areas?

A. Configuration management
B. Integrated change control

C. Risk analysis

D. Project change control system

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Integrated change control is responsible for evaluating a proposed change and determining its impact on all areas of the project: scope, time, cost, quality, human resources, communication, risk, and procurement.
Answer: D is incorrect. The project change control system defines the workflow and approval process for proposed changes to the project scope, time, cost, and contracts. Answer: A is incorrect. Configuration management defines the management, control, and documentation of the features and functions of the project's product. Answer: C is incorrect. Risk analysis is not responsible for reviewing the change aspects for the entire project.

QUESTION 161
While developing obscure risk scenarios, what are the requirements of the enterprise? Each correct answer represents a part of the solution. Choose two.

A. Have capability to cure the risk events

B. Have capability to recognize an observed event as something wrong

C. Have sufficient number of analyst

D. Be in a position that it can observe anything going wrong

Correct Answer: BD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The enterprise must consider risk that has not yet occurred and should develop scenarios around unlikely, obscure or non-historical events.
Such scenarios can be developed by considering two things:
Visibility
Recognition
For the fulfillment of this task enterprise must:
Be in a position that it can observe anything going wrong Have the capability to recognize an observed event as something wrong Answer: C and A are incorrect. These are not the direct requirements for developing obscure risk scenarios, like curing risk events comes under process of risk management. Hence capability of curing risk event does not lay any impact on the process of development of risk scenarios.

QUESTION 162
You are the project manager of GHT project. During the data extraction process you evaluated the total number of transactions per year by multiplying the monthly

average by twelve. This process of evaluating total number of transactions is known as?

A. Duplicates test
B. Controls total
C. Simplistic and ineffective
D. Reasonableness test

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Reasonableness tests make certain assumptions about the information as the basis for more elaborate data validation tests.
Answer: A is incorrect. The duplicate test does not identify duplicate transactions; rather it identifies and confirms the validity of duplicates. Answer: C is incorrect. As compared to simplistic, the reasonableness test is a valid foundation for more elaborate data validation tests. Answer: B is incorrect. The control total test does not ensure that all transactions have been extracted, but only ensures that the data are complete.

QUESTION 163
Who is at the BEST authority to develop the priorities and identify what risks and impacts would occur if there were loss of the organization's private information?

A. External regulatory agencies
B. Internal auditor
C. Business process owners
D. Security management

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Business process owners are in best position to judge the risks and impact, as they are most knowledgeable concerning their systems. Hence they are most suitable for developing and identifying risks on business.
Answer: B, D, and A are incorrect. Internal auditors, security managers, external regulators would not understand the impact on business to the extent that business owners could. Hence business owner is the best authority.

QUESTION 164
You are the project manager for TTP project. You are in the Identify Risks process. You have to create the risk register. Which of the following are included in the risk register? Each correct answer represents a complete solution. Choose two.

A. List of potential responses

B. List of key stakeholders

C. List of mitigation techniques

D. List of identified risks

Correct Answer: AD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk register primarily contains the following:
List of identified risks: A reasonable description of the identified risks is noted in the risk register. The description includes event, cause, effect, impact related to the risks identified. In addition to the list of identified risks, the root causes of those risks may appear in the risk register.
List of potential responses: Potential responses to a risk may be identified during the Identify Risks process. These responses are useful as inputs to the Plan Risk Responses process. Answer: C is incorrect. Risk register do contain the summary of mitigation, but only after the applying risk response. Here in this scenario you are in risk identification phase, hence mitigation techniques cannot be documented at this situation. Answer: B is incorrect. This is not valid content of risk register.
A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains:
A description of the risk
The impact should this event actually occur
The probability of its occurrence
Risk Score (the multiplication of Probability and Impact) A summary of the planned response should the event occur A summary of the mitigation (the actions taken in advance to reduce the probability and/or impact of the event) Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved.

QUESTION 165
You work as a project manager for BlueWell Inc. You are about to complete the quantitative risk analysis process for your project. You can use three available tools and techniques to complete this process. Which one of the following is NOT a tool or technique that is appropriate for the quantitative risk analysis process?

A. Data gathering and representation techniques

B. Expert judgment

C. Quantitative risk analysis and modeling techniques

D. Organizational process assets

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:

Explanation:
Organizational process asset is not a tool and technique, but an input to the quantitative risk analysis process. Quantitative Risk Analysis is a process to assess the probability of achieving particular project objectives, to quantify the effect of risks on the whole project objective, and to prioritize the risks based on the impact to overall project risk. Quantitative Risk Analysis process analyzes the affect of a risk event deriving a numerical value. It also presents a quantitative approach to build decisions in the presence of uncertainty. The inputs for Quantitative Risk Analysis are :
Organizational process assets
Project Scope Statement
Risk Management Plan
Risk Register
Project Management Plan
Answer: A is incorrect. Data gathering and representation technique is a tool and technique for the quantitative risk analysis process.
Answer: C is incorrect. Quantitative risk analysis and modeling techniques is a tool and technique for the quantitative risk analysis process. Answer: B is incorrect. Expert judgment is a tool and technique for the quantitative risk analysis process.

QUESTION 166
Which of the following is the PRIMARY requirement before choosing Key performance indicators of an enterprise?

A. Determine size and complexity of the enterprise
B. Prioritize various enterprise processes
C. Determine type of market in which the enterprise operates
D. Enterprise must establish its strategic and operational goals

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Key Performance Indicators is a set of measures that a company or industry uses to measure and/or compare performance in terms of meeting their strategic and operational goals. KPIs vary with company to company, depending on their priorities or performance criteria. A company must establish its strategic and operational goals and then choose their KPIs which can best reflect those goals. For example, if a software company's goal is to have the fastest growth in its industry, its main performance indicator may be the measure of its annual revenue growth.
Answer: B is incorrect. This is not the valid answer. Answer: A is incorrect. Determination of size and complexity of the enterprise is the selection criteria of the KRI, not KPI. KPI does not have any relevancy with size and complexity of the enterprise.
Answer: C is incorrect. Type of market in which the enterprise is operating do not affect the selection of KPIs.

QUESTION 167
You are the project manager of project for a client. The client has promised your company a bonus, if the project is completed early. After studying the project work, you elect to crash the project in order to realize the early end date. This is an example of what type of risk response?

A. Negative risk response, because crashing will add risks.

B. Positive risk response, as crashing is an example of enhancing.
C. Positive risk response, as crashing is an example of exploiting.
D. Negative risk response, because crashing will add costs.

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
This is a positive risk response, as crashing is an example of enhancing. You are enhancing the probability of finishing the project early to realize the reward of bonus. Enhancing doesn't ensure positive risks, but it does increase the likelihood of the event. Answer: D is incorrect. Crashing does add costs, but in this instance, crashing is an example of the positive risk response of enhancing.
Answer: A is incorrect. Crashing is a positive risk response. Generally, crashing doesn't add risks and is often confused with other predominant schedule compression techniques of fast tracking - which does add risks.
Answer: C is incorrect. This isn't an example of exploiting. Exploiting is an action to take advantage of a positive risk response that will happen.

QUESTION 168
Judy has identified a risk event in her project that will have a high probability and a high impact. Based on the requirements of the project, Judy has asked to change the project scope to remove the associated requirement and the associated risk. What type of risk response is this?

A. Exploit
B. Not a risk response, but a change request
C. Avoidance
D. Transference

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk avoidance involves changing the project management plan to eliminate the threat entirely. The project manager may also isolate the project objectives from the risk's impact or change the objective that is in jeopardy. Examples of this include extending the schedule, changing the strategy, or reducing the scope. The most radical avoidance strategy is to shut down the project entirely. Some risks that arise early in the project can be avoided by clarifying requirements, obtaining information, improving communication, or acquiring expertise.
Answer: A is incorrect. Exploit risk response is used for positive risk or opportunity, not for negative risk.
Answer: D is incorrect. Transference allows the risk to be transferred, not removed from the project, to a third party. Transference usually requires a contractual relationship with the third party.
Answer: B is incorrect. This risk response does require a change request, in some instances, but it's the avoidance risk response and not just a change request.

QUESTION 169
You are the risk professional of your enterprise. You have performed cost and benefit analysis of control that you have adopted. What are all the benefits of performing cost and benefit analysis of control? Each correct answer represents a complete solution. Choose three.

A. It helps in determination of the cost of protecting what is important
B. It helps in taking risk response decisions
C. It helps in providing a monetary impact view of risk
D. It helps making smart choices based on potential risk mitigation costs and losses

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:

QUESTION 170
You are the project manager of GHT project. You want to perform post-project review of your project. What is the BEST time to perform post-project review by you and your project development team to access the effectiveness of the project?

A. Project is completed and the system has been in production for a sufficient time period
B. During the project
C. Immediately after the completion of the project
D. Project is about to complete

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The project development team and appropriate end users perform a post-project review jointly after the project has been completed and the system has been in production for a sufficient time period to assess its effectiveness. Answer: C is incorrect. It is not done immediately after the completion of the project as its effectiveness cannot be measured until the system has been in production for certain time period.
Answer: B is incorrect. The post-project review of project for accessing effectiveness cannot be done during the project as effectiveness can only evaluated after setting the project in process of production.
Answer: D is incorrect. Post-project review for evaluating the effectiveness of the project can only be done after the completion of the project and the project is in production phase.

QUESTION 171
What are the steps that are involved in articulating risks? Each correct answer represents a complete solution. Choose three.

A. Identify business opportunities.
B. Identify the response
C. Communicate risk analysis results and report risk management activities and the state of compliance.
D. Interpret independent risk assessment findings.

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Following are the tasks that are involved in articulating risk:
Communicate risk analysis results.
Report risk management activities and the state of compliance.
Interpret independent risk assessment findings.
Identify business opportunities.

QUESTION 172
What are the requirements of effectively communicating risk analysis results to the relevant stakeholders? Each correct answer represents a part of the solution. Choose three.

A. The results should be reported in terms and formats that are useful to support business decisions
B. Communicate only the negative risk impacts of events in order to drive response decisions
C. Communicate the risk-return context clearly
D. Provide decision makers with an understanding of worst-case and most probable scenarios

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The result of risk analysis process is being communicated to relevant stakeholders. The steps that are involved in communication are:
The results should be reported in terms and formats that are useful to support business decisions. Coordinate additional risk analysis activity as required by decision makers, like report rejection and scope adjustment. Communicate the risk-return context clearly, which include probabilities of loss and/or gain, ranges, and confidence levels (if possible) that enable management to balance risk-return. Identify the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process. Provide decision makers with an

understanding of worst-case and most probable scenarios, due diligence exposures and significant reputation, legal or regulatory considerations. Answer: B is incorrect. Both the negative and positive risk impacts are being communicated to relevant stakeholders. Identify the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process.

QUESTION 173
Which among the following is the MOST crucial part of risk management process?

A. Risk communication
B. Auditing
C. Risk monitoring
D. Risk mitigation

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk communication is a critical part in the risk management process. People are naturally uncomfortable talking about risk and tend to put off admitting that risk is involved and communicating about issues; incidents; and; eventually, even crises. If risk is to be managed and mitigated, it must first be discussed and effectively communicated throughout an enterprise.
Answer: D is incorrect. Risk mitigation is one of the phases of risk management process for effective mitigation of risk it should be first communicated throughout an enterprise. Answer: B is incorrect. Auditing is done to test the overall risk management process and the planned risk responses. So it is the very last phase after completion of risk management process.
Answer: C is incorrect. Risk monitoring is the last phase to complete risk management process, and for proper management of risk it should be communicated properly. Hence risk communication is the most crucial step.

QUESTION 174
Which of the following is a key component of strong internal control environment?

A. RMIS
B. Segregation of duties
C. Manual control
D. Automated tools

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

Explanation:
Segregation of duties (SOD) is a key component to maintaining a strong internal control environment because it reduces the risk of fraudulent transactions. When duties for a business process or transaction are segregated it becomes more difficult for fraudulent activity to occur because it would involve collusion among several employees. Answer: D is incorrect. It is not directly related in maintaining strong internal control environment. The automated tools are typically used to address SOD and also to provide the enterprise with reporting functionality on SOD violations (i.e., detective controls) and to put in place preventive controls. Answer: C is incorrect. Manual controls usually not form strong internal control environment. By not automating SOD controls, there is, potentially, the issue of these controls becoming a barrier in serving the customer. As manual authorizations are often time consuming and require another step in any business process, this takes time away from serving the customer. Automated compliance solutions aim to provide enterprises with timely and efficient internal controls that do not disrupt their normal business process. Answer: A is incorrect. An RMIS can be a very effective tool in monitoring all risk factors that impact the enterprise. The danger is that many important classes of risk may be omitted from consideration by the system. hence it doesn't ensure strong internal control environment.

QUESTION 175
You are the project manager of the NKJ Project for your company. The project's success or failure will have a significant impact on your organization's profitability for the coming year. Management has asked you to identify the risk events and communicate the event's probability and impact as early as possible in the project. Management wants to avoid risk events and needs to analyze the cost-benefits of each risk event in this project. What term is assigned to the low-level of stakeholder tolerance in this project?

A. Mitigation-ready project management
B. Risk avoidance
C. Risk utility function
D. Risk-reward mentality

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk utility function is assigned to the low-level of stakeholder tolerance in this project. The risk utility function describes a person's or organization's willingness to accept risk. It is synonymous with stakeholder tolerance to risk.
Risk utility function facilitates the selection and acceptance of risk and provides opportunity to merge the approach with setting thresholds
of risk acceptability and using utility-risk ratios if necessary. Answer: B is incorrect. Risk avoidance is a risk response to avoid negative risk events. Answer: A is incorrect. This is not a valid project management and risk management term. Answer: D is incorrect. Risk-reward describes the balance between accepting risks and the expected reward for the risk event. Risk-reward mentality is not a valid project management term.

QUESTION 176
How residual risk can be determined?

A. By determining remaining vulnerabilities after countermeasures are in place.
B. By transferring all risks.

C. By threat analysis

D. By risk assessment

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
All risks are determined by risk assessment, regardless whether risks are residual or not. Answer: A is incorrect. Determining remaining vulnerabilities after countermeasures are in place says nothing about threats, therefore risk cannot be determined. Answer: C is incorrect. Risk cannot be determined by threat analysis alone, regardless whether it is residual or not.
Answer: B is incorrect. Transferring all the risks in not relevant to determining residual risk.
It is one of the method of risk management.

QUESTION 177
Which of the following are the MOST important risk components that must be communicated among all the stakeholders?
Each correct answer represents a part of the solution. Choose three.

A. Various risk response used in the project

B. Expectations from risk management

C. Current risk management capability

D. Status of risk with regard to IT risk

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The broad array of information and the major types of IT risk information that should be communicated are as follows:
Expectations from risk management: They include risk strategy, policies, procedures, awareness training, uninterrupted reinforcement of principles, etc. This essential communication drives all subsequent efforts on risk management and sets the overall expectations from risk management.
Current risk management capability: This allows monitoring of the status of the risk management engine in the enterprise. It is a key indicator for effective risk management and has predictive value for how well the enterprise is managing risk and reducing exposure. Status with regard to IT risk: This describes the actual status with regard to IT risk including information of risk profile of the enterprise, Key risk indicators (KRIs) to support management reporting on risk, event-loss data, root cause of loss events and options to mitigate risk.
Answer: A is incorrect. Risk response is only communicated to some of the stakeholders not all, as it is irrelevant for them. It is not communicated to the stakeholders of the project like project sponsors, etc.

QUESTION 178
You work as a project manager for BlueWell Inc. You are involved with the project team on the different risk issues in your project. You are using the applications of IRGC model to facilitate the understanding and managing the rising of the overall risks that have impacts on the economy and society. One of your team members wants to know that what the need to use the IRGC is. What will be your reply?

A. IRGC models aim at building robust, integrative inter-disciplinary governance models for emerging and existing risks.
B. IRGC is both a concept and a tool.
C. IRGC addresses the development of resilience and the capacity of organizations and people to face unavoidable risks.
D. IRGC addresses understanding of the secondary impacts of a risk.

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
IRGC is aimed at building robust, integrative inter-disciplinary governance models for emerging and existing risks.
The International Risk Governance Council (IRGC) is a self-governing organization whose principle is to facilitate the understanding and managing the rising overall risks that have impacts on the economy and society, human health and safety, the environment at large. IRGC's effort is to build and develop concepts of risk governance, predict main risk issues and present risk governance policy recommendations for the chief decision makers. IRGC mainly emphasizes on rising, universal risks for which governance deficits exist. Its goal is to present recommendations for how policy makers can correct them. IRGC models at constructing strong, integrative inter-disciplinary governance models for up-coming and existing risks.
Answer: B is incorrect. As IRGC is aimed at building robust, integrative inter-disciplinary governance models for emerging and existing risks, so it is the best answer for this options D and C are incorrect. Risk governance addresses understanding of the secondary impacts of a risk, the development of resilience and the capacity of organizations and people to face unavoidable risks.

QUESTION 179
You are elected as the project manager of GHT project. You are in project initialization phase and are busy in defining requirements for your project. While defining requirements you are describing how users will interact with a system. Which of the following requirements are you defining here?

A. Technical requirement
B. Project requirement
C. Functional requirement
D. Business requirement

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:

Explanation:
While defining requirements, there is need to define three requirements of the project- Business requirement, Functional requirement, and
Technical requirement
Functional requirements and use case models describe how users will interact with a system. Therefore here in this stem you are defining the functional requirement of the project. Answer: D is incorrect. Business requirements contain descriptions of what a system should do.
Answer: A is incorrect. Technical requirements and design specifications and coding specifications describe how the system will interact, conditions under which the system will operate and the information criteria the system should meet. Answer: B is incorrect. Business requirement, Functional requirement, and Technical requirement come under project requirement. In this stem it is particular defining the functional requirement, hence this is not the best answer.

QUESTION 180
While considering entity-based risks, which dimension of the COSO ERM framework is being referred?

A. Organizational levels
B. Risk components
C. Strategic objectives
D. Risk objectives

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The organizational levels of the COSO ERM framework describe the subsidiary, business unit, division, and entity-levels of aspects of risk solutions. Answer: C is incorrect. Strategic objectives includes strategic, operational, reporting, and compliance risks; and not entity-based risks.
Answer: B is incorrect. Risk components includes Internal Environment, Objectives settings, Event identification, Risk assessment, Risk response, Control activities, Information and communication, and monitoring.
Answer: D is incorrect. This is not valid answer.

QUESTION 181
You are the project manager for Bluewell Inc. You are studying the documentation of project plan. The documentation states that there are twenty-five stakeholders with the project. What will be the number of communication channel s for the project?

A. 20
B. 100
C. 50
D. 300

Correct Answer: D
Section: Volume C

Explanation

Explanation/Reference:
Explanation:
Communication channels are paths of communication with stakeholders in a project. The number of communication channels shows the complexity of a project's communication and can be derived through the formula shown below:
Total Number of Communication Channels = n (n-1)/2
Where n is the number of stakeholders. Hence, a project having five stakeholders will have ten communication channels. Putting the value of the number of stakeholders in the formula will provide the number of communication channels.
Hence,
Number of communication channel = (n (n-1)) / 2
= (25 (25-1)) / 2
= (25 x 24) / 2
= 600 / 2
= 300
Answer: A, C, and B are incorrect.
These are not valid number of communication channels for the given scenario.

QUESTION 182
Which of the following are the common mistakes while implementing KRIs? Each correct answer represents a complete solution. Choose three.

A. Choosing KRIs that are difficult to measure
B. Choosing KRIs that has high correlation with the risk
C. Choosing KRIs that are incomplete or inaccurate due to unclear specifications
D. Choosing KRIs that are not linked to specific risk

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
A common mistake when implementing KRIs other than selecting too many KRIs includes choosing KRIs that are:
Not linked to specific risk
Incomplete or inaccurate due to unclear specifications Too generic
Difficult to aggregate, compare and interpret
Difficult to measure
Answer: B is incorrect. For ensuring high reliability of the KRI, The indicator must possess a high correlation with the risk and be a good predictor or outcome measure. Hence KRIs are chosen that has high correlation with the risk.

QUESTION 183

Which of the following control audit is performed to assess the efficiency of the productivity in the operations environment?

A. Operational
B. Financial
C. Administrative
D. Specialized

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The administrative audit is used to assess the efficiency of the productivity in the operations environment.
Answer: B is incorrect. Audits that assesses the correctness of financial statements is called financial audit.
Answer: A is incorrect. It evaluates the internal control structure of process of functional area.
Answer: D is incorrect. They are the IS audits with specific intent to examine areas, such as processes, services, or technologies, usually by third party auditors.

QUESTION 184
Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months.
Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?

A. Project risk management has been concluded with the project planning.
B. Project risk management happens at every milestone.
C. Project risk management is scheduled for every month in the 18-month project.
D. At every status meeting the project team project risk management is an agenda item.

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk management is an ongoing project activity. It should be an agenda item at every project status meeting.
Answer: B is incorrect. Milestones are good times to do reviews, but risk management should happen frequently.
Answer: C is incorrect. This answer would only be correct if the project has a status meeting just once per month in the project.
Answer: A is incorrect. Risk management happens throughout the project as does project planning.

QUESTION 185

You are the project manager of the NGQQ Project for your company. To help you communicate project status to your stakeholders, you are going to create a stakeholder register. All of the following information should be included in the stakeholder register except for which one?

A. Stakeholder management strategy
B. Assessment information of the stakeholders' major requirements, expectations, and potential influence
C. Identification information for each stakeholder
D. Stakeholder classification of their role in the project

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The stakeholder management strategy is generally not included in the stakeholder registry because it may contain sensitive information that should not be shared with project team members or certain other individuals that could see the stakeholder register. The stakeholder register is a project management document that contains a list of the stakeholders associated with the project. It assesses how they are involved in the project and identifies what role they play in the organization. The information in this document can be very perceptive and is meant for limited exchange only. It also contains relevant information about the stakeholders, such as their requirements, expectations, and influence on the project. Answer: C, B, and D are incorrect. Stakeholder identification, Assessment information, and Stakeholder classification should be included in the stakeholder register.

QUESTION 186
Della works as a project manager for Tech Perfect Inc. She is studying the documentation of planning of a project. The documentation states that there are twenty-eight stakeholders with the project. What will be the number of communication channels for the project?

A. 250
B. 28
C. 378
D. 300

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
According to the twenty- eight stakeholders. Communication channels are paths of communication with stakeholders in a project. The number of communication channels shows the complexity of a project's communication and can be derived through the formula shown below:
Total Number of Communication Channels = n (n-1)/2
Where n is the number of stakeholders. Hence, a project having five stakeholders will have ten communication channels. Putting the value of the number of

stakeholders in the formula will provide the number of communication channels. Putting the value of the number of stakeholders in the formula will provide the number of communication channels:
Number of communication channel = (n (n-1)) / 2
= (28 (28-1)) / 2
= (28 x 27) / 2
= 756 / 2
= 378

QUESTION 187
Shawn is the project manager of the HWT project. In this project Shawn's team reports that they have found a way to complete the project work cheaply than what was originally estimated earlier. The project team presents a new software that will help to automate the project work. While the software and the associated training costs $25,000 it will save the project nearly $65,000 in total costs. Shawn agrees to the software and changes the project management plan accordingly. What type of risk response had been used by him?

A. Avoiding
B. Accepting
C. Exploiting
D. Enhancing

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
A risk event is been exploited so as to identify the opportunities for positive impacts. 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: B is incorrect. Accepting is a risk response that is appropriate for positive or negative risk events. It does not pursue the risk, but documents the event and allows the risk to happen. Often acceptance is used for low probability and low impact risk events. Answer: A is incorrect. To avoid a risk means to evade it altogether, eliminate the cause of the risk event, or change the project plan to protect the project objectives from the risk event. Answer: D is incorrect. Enhancing is a positive risk response that aims to increase the probability and/or impact of the risk event.

QUESTION 188
Which among the following is the BEST reason for defining a risk response?

A. To eliminate risk from the enterprise
B. To ensure that the residual risk is within the limits of the risk appetite and tolerance
C. To overview current status of risk
D. To mitigate risk

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The purpose of defining a risk response is to ensure that the residual risk is within the limits of the risk appetite and tolerance of the enterprise. Risk response is based on selecting the correct, prioritized response to risk, based on the level of risk, the enterprise's risk tolerance and the cost or benefit of the particular risk response option. Answer: A is incorrect. Risk cannot be completely eliminated from the enterprise. Answer: D is incorrect. Mitigation of risk is itself the risk response process, not the reason behind this.
Answer: C is incorrect. This is not a valid answer.

QUESTION 189
Which of the following is the BEST defense against successful phishing attacks?

A. Intrusion detection system
B. Application hardening
C. End-user awareness
D. Spam filters

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing attacks are a type of to social engineering attack and are best defended by end-user awareness training.
Answer: B is incorrect. Application hardening does not protect against phishing attacks since phishing attacks generally use e-mail as the attack vector, with the end-user as the vulnerable point, not the application.
Answer: D is incorrect. Certain highly specialized spam filters can reduce the number of phishing e-mails that reach the inboxes of user, but they are not as effective in addressing phishing attack as end-user awareness.
Answer: A is incorrect. An intrusion detection system does not protect against phishing attacks since phishing attacks usually do not have a particular pattern or unique signature.

QUESTION 190
Which of the following laws applies to organizations handling health care information?

A. GLBA

B. HIPAA
C. SOX
D. FISMA

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
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: C is incorrect. SOX designed to hold executives and board members personally responsible for financial data.
Answer: A is incorrect. GLBA is not used for handling health care information. Answer: D is incorrect. FISMA ensures protection of data of federal agencies.

QUESTION 191
Mike is the project manager of the NNP Project for his organization. He is working with his project team to plan the risk responses for the NNP Project. Mike would like the project team to work together on establishing risk thresholds in the project. What is the purpose of establishing risk threshold?

A. It is a study of the organization's risk tolerance.
B. It is a warning sign that a risk event is going to happen.
C. It is a limit of the funds that can be assigned to risk events.
D. It helps to identify those risks for which specific responses are needed.

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk threshold helps to identify those risks for which specific responses are needed.

QUESTION 192
You work as a project manager for BlueWell Inc. You are preparing to plan risk responses for your project with your team. How many risk response types are available for a negative risk event in the project?

A. 5
B. 7
C. 1
D. 4

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Four risk response options are there to deal with negative risks or threats on the project objectives- avoid, transfer, mitigate, and accept.
Risk avoidance
Risk mitigation
Risk transfer
Risk acceptance
Answer: A, C, and B are incorrect. These are incorrect choices as only 4 risk response are available to deal with negative risks.

QUESTION 193
You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

A. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.
B. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
C. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.
D. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process.
Answer: B is incorrect. This is actually the definition of qualitative risk analysis. Answer: A is incorrect. While somewhat true, this statement does not completely define the quantitative risk analysis process.
Answer: D is incorrect. This is not a valid statement about the quantitative risk analysis process. Risk response planning is a separate project management process.

QUESTION 194
You are the project manager of your enterprise. You have identified new threats, and then evaluated the ability of existing controls to mitigate risk associated with new threats. You noticed that the existing control is not efficient in mitigating these new risks. What are the various steps you could take in this case?
Each correct answer represents a complete solution. Choose all that apply.

A. Education of staff or business partners
B. Deployment of a threat-specific countermeasure
C. Modify of the technical architecture
D. Apply more controls

Correct Answer: ABC
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
As new threats are identified and prioritized in terms of impact, the first step is to evaluate the ability of existing controls to mitigate risk associated with new threats and if it does not work then in that case facilitate the:
Modification of the technical architecture
Deployment of a threat-specific countermeasure
Implementation of a compensating mechanism or process until mitigating controls are developed
Education of staff or business partners
Answer: D is incorrect. Applying more controls is not the good solution. They usually complicate the condition.

QUESTION 195
Which of the following risks is associated with not receiving the right information to the right people at the right time to allow the right action to be taken?

A. Relevance risk
B. Integrity risk
C. Availability risk

D. Access risk

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Relevance risk is the risk associated with not receiving the right information to the right people (or process or systems) at the right time to allow the right action to be taken. Answer: D is incorrect. The risk that confidential or private information may be disclosed or made available to those without appropriate authority is termed as access or security risk. An aspect of this risk is non-compliance with local, national and international laws related to privacy and protection of personal information.
Answer: B is incorrect. The risk that data cannot be relied on because they are unauthorized, incomplete or inaccurate is termed as integrity risk. Answer: C is incorrect. The risk of loss of service or that data is not available when needed is referred as availability risk.

QUESTION 196
Kelly is the project manager of the NNQ Project for her company. This project will last for one year and has a budget of $350,000. Kelly is working with her project team and subject matter experts to begin the risk response planning process. What are the two inputs that Kelly would need to begin the plan risk response process?

A. Risk register and the results of risk analysis
B. Risk register and the risk response plan
C. Risk register and power to assign risk responses
D. Risk register and the risk management plan

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The only two inputs for the risk response planning are the risk register and the risk management plan.
The plan risk response project management process aims to reduce the threats to the project objectives and to increase opportunities. It follows the perform qualitative risk analysis process and perform quantitative risk analysis process. Plan risk response process includes the risk response owner to take the job for each agreed-to and funded risk response. This process addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget. The inputs to the plan risk response process are as follows:
Risk register
Risk management plan
Answer: B is incorrect. Kelly will not need the risk response plan until monitoring and controlling the project.
Answer: C is incorrect. The results of risk analysis will help Kelly prioritize the risks, but this information will be recorded in the risk register.
Answer: D is incorrect. Kelly needs the risk register and the risk management plan as the input. The power to assign risk responses is not necessarily needed by

Kelly.

QUESTION 197
Tom works as a project manager for BlueWell Inc. He is determining which risks can affect the project. Which of the following inputs of the identify risks process is useful in identifying risks, and provides a quantitative assessment of the likely cost to complete the scheduled activities?

A. Activity duration estimates
B. Risk management plan
C. Cost management plan
D. Activity cost estimates

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The activity cost estimates review is valuable in identifying risks as it provides a quantitative assessment of the expected cost to complete the scheduled activities and is expressed as a range, with a width of the range indicating the degrees of risk. Answer: B is incorrect. This is the output of plan risk management process. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix.
Answer: A is incorrect. The activity duration estimates review is valuable in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk.
Answer: C is incorrect. The cost management plan sets how the costs on a project are managed during the project's lifecycle. It defines the format and principles by which the project costs are measured, reported, and controlled. The cost management plan identifies the person responsible for managing costs, those who have the authority to approve changes to the project or its budget, and how cost performance is quantitatively calculated and reported upon.

QUESTION 198
Which of the following baselines identifies the specifications required by the resource that meet the approved requirements?

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

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

Explanation:
Allocated baseline identifies the specifications that meet the approved requirements. Answer: A is incorrect. Functional baseline identifies the initial specifications before any changes are made.
Answer: C is incorrect. Product baseline identifies the minimal specification required by the resource to meet business outcomes.
Answer: D is incorrect. Developmental baseline identifies the state of the resources as it is developed to meet or exceed expectations and requirements.

QUESTION 199
Which of the following nodes of the decision tree analysis represents the start point of decision tree?

A. Decision node
B. End node
C. Event node
D. Root node

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Root node is the starting node in the decision tree. Answer: C is incorrect. Event node represents the possible uncertain outcomes of a risky decision, with at least two nodes to illustrate the positive and negative range of events. Answer: A is incorrect. Decision nodes represents the choice available to the decision maker, usually between a risky choice and its non-risky counterpart. Answer: B is incorrect. End node represents the outcomes of risk and decisions.

QUESTION 200
You are the project manager of the NHH Project. You are working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document do you and your team is creating in this scenario?

A. Project plan
B. Resource management plan
C. Project management plan
D. Risk management plan

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:

The risk management plan, part of the comprehensive management plan, defines how risks will be identified, analyzed, monitored and controlled, and even responded to. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix.
Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for project execution.
Answer: C is incorrect. The project management plan is a comprehensive plan that communicates the intent of the project for all project management knowledge areas. Answer: A is incorrect. The project plan is not an official PMBOK project management plan. Answer: B is incorrect. The resource management plan defines the management of project resources, such as project team members, facilities, equipment, and contractors.

QUESTION 201
Where are all risks and risk responses documented as the project progresses?

A. Risk management plan
B. Project management plan
C. Risk response plan
D. Risk register

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
All risks, their responses, and other characteristics are documented in the risk register. As the project progresses and the conditions of the risk events change, the risk register should be updated to reflect the risk conditions.
Answer: A is incorrect. The risk management plan addresses the project management's approach to risk management, risk identification, analysis, response, and control. Answer: C is incorrect. The risk response plan only addresses the planned risk responses for the identified risk events in the risk register.
Answer: B is incorrect. The project management plan is the overarching plan for the project, not the specifics of the risk responses and risk identification.

QUESTION 202
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

A. Transference
B. Mitigation
C. Avoidance
D. Exploit

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
When you are hiring a third party to own risk, it is known as transference risk response. Risk transfer means that impact of risk is reduced by transferring or otherwise sharing a portion of the risk with an external organization or another internal entity. Transfer of risk can occur in many forms but is most effective when dealing with financial risks. Insurance is one form
of risk transfer.
Answer: B is incorrect. The act of spending money to reduce a risk probability and impact is known as mitigation.
Answer: D is incorrect. Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Answer: C is incorrect. When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

QUESTION 203
John works as a project manager for BlueWell Inc. He is determining which risks can affect the project. Which of the following inputs of the identify risks process is useful in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk?

A. Activity duration estimates
B. Activity cost estimates
C. Risk management plan
D. Schedule management plan

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The activity duration estimates review is valuable in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk.
Answer: B is incorrect. The activity cost estimates review is valuable in identifying risks as it provides a quantitative assessment of the expected cost to complete scheduled activities and is expressed as a range, with a width of the range indicating the degrees of risk. Answer: D is incorrect. It describes how the schedule contingencies will be reported and assessed.
Answer: C is incorrect. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix.

QUESTION 204
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

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:
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
Answer: A is incorrect. Someone sees company's secret formula or password comes under loss of confidentiality.

QUESTION 205
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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
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.
Answer: B is incorrect. Review of the existing IT environment is also useful and necessary but is not the first step that needs to be undertaken. Answer: D is incorrect. The present IT budget is just one of the components of the strategic plan.
Answer: A is incorrect. The IT strategic plan exists to support the enterprise's strategic plan but is not solely considered while designing information system control.

QUESTION 206
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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: A is incorrect. This is the consequence of poor risk communication, not the inhibitor of effective communication.
Answer: D is incorrect. 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.
Answer: B is incorrect. . This is the consequence of poor risk communication, not the inhibitor of effective communication.

QUESTION 207
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.

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Low-impact, low-probability risks can be added to the low priority risk watch list. Answer: B is incorrect. 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.
Answer: A is incorrect. These risks are not dismissed; they are still documented on the low priority risk watch list.
Answer: D is incorrect. Not every risk demands a risk response, so this choice is incorrect.

QUESTION 208
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

Correct Answer: A
Section: Volume C
Explanation

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

QUESTION 209
What are the functions of audit and accountability control? Each correct answer represents a complete solution. Choose all that apply.

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

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
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.
Answer: B is incorrect. 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 210
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

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
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.
Answer: C and A are incorrect. 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 followingtwo 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. Answer: D is incorrect. 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 211
What is the value of exposure factor if the asset is lost completely?

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

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: B, D, and C are incorrect. These are not the values of exposure factor for zero assets.

QUESTION 212
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

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: C is incorrect. Opportunistic is not a valid risk response. Answer: B is incorrect. This is an example of a positive risk, but positive is not a risk response.
Answer: A is incorrect. Enhancing is a positive risk response that describes actions taken to increase the odds of a risk event to happen.

QUESTION 213
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

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: C, A, and B are incorrect. These are wrong formulas and are not used in quantitative risk assessment.

QUESTION 214
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

Correct Answer: ABD
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: C is incorrect. Enterprise having risk management capability maturity level 5 requires continuous improvement of risk management skills, based on clearly defined personal and enterprise goals.

QUESTION 215
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)

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: C is incorrect. 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.
Answer: B is incorrect. 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.
Answer: D is incorrect. CRO is the individual who oversees all aspects of risk management across the enterprise. He/she is responsible for analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.

QUESTION 216
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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: B is incorrect. Threats are circumstances or events with the potential to cause harm to information resources. This scenario does not describe a threat. Answer: A is incorrect. Probabilities represent the likelihood of the occurrence of a threat, and this scenario does not describe a probability. Answer: D is incorrect. Impacts represent the outcome or result of a threat exploiting a vulnerability. The stem does not describe an impact.

QUESTION 217
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

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
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.
Answer: C is incorrect. Training can increase user awareness of the information security policy, but is less effective than periodic auditing. Answer: A is incorrect. Penetration testing can identify security vulnerability, but cannot ensure information compliance.
Answer: B is incorrect. 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 comply with the enterprise's information security policy.

QUESTION 218
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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
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.
Answer: B is incorrect. Quick win is very effective and efficient response that addresses medium to high risk. But in this the response does not require large

investments. Answer: A is incorrect. It addresses costly risk response to a low risk. But here the response is less costly than that of business case to be made. Answer: D is incorrect. 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 219
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.

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: B is incorrect. 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. Answer: A is incorrect. 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.
Answer: C is incorrect. 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 220
Which of following is NOT used for measurement of Critical Success Factors of the project?

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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Answer: A, B, and D are incorrect. Productivity, quality and customer service are used for evaluating critical service factor of any particular project.

QUESTION 221
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.

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
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. Answer: A, D, and B are incorrect. 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 222
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

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
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 oppourtunities 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.
Answer: D is incorrect. 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.
Answer: A is incorrect. 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.
Answer: B is incorrect. 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.

QUESTION 223
What is the MAIN purpose of designing risk management programs?

A. To reduce the risk to a level that the enterprise is willing to accept
B. To reduce the risk to the point at which the benefit exceeds the expense
C. To reduce the risk to a level that is too small to be measurable
D. To reduce the risk to a rate of return that equals the current cost of capital

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk cannot be removed completely from the enterprise; it can only be reduced to a level that an organization is willing to accept. Risk management programs are hence designed to accomplish the task of reducing risks.
Answer: B is incorrect. Depending on the risk preference of an enterprise, it may or may not choose to pursue risk mitigation to the point at which benefit equals or exceeds the expense. Hence this is not the primary objective of designing the risk management program. Answer: C is incorrect. Reducing risk to a level too small to measure is not practical and is often cost-prohibitive.
Answer: D is incorrect. Reducing risks to a specific return ignores the qualitative aspects of the risk which should also be considered.

QUESTION 224
Which of the following is the priority of data owners when establishing risk mitigation method?

A. User entitlement changes
B. Platform security
C. Intrusion detection
D. Antivirus controls

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Data owners are responsible for assigning user entitlement changes and approving access to the systems for which they are responsible.
Answer: C, B, and D are incorrect. Data owners are not responsible for intrusion detection, platform security or antivirus controls.
These are the responsibilities of data custodians.

QUESTION 225
What type of policy would an organization use to forbid its employees from using organizational e-mail for personal use?

A. Anti-harassment policy
B. Acceptable use policy
C. Intellectual property policy
D. Privacy policy

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
An acceptable use policy is a set of rules applied by the owner/manager of a network, website or large computer system that restrict the ways in which the network site or system may be used. Acceptable Use Policies are an integral part of the framework of information security policies.
Answer: D is incorrect. Privacy policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data.
Answer: C and A are incorrect. These two policies are not related to Information system security.

QUESTION 226
Wendy has identified a risk event in her project that has an impact of $75,000 and a 60 percent chance of happening. Through research, her project team learns that the risk impact can actually be reduced to just $15,000 with only a ten percent chance of occurring. The proposed solution will cost $25,000. Wendy agrees to the $25,000 solution. What type of risk response is this?

A. Mitigation
B. Avoidance
C. Transference
D. Enhancing

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk mitigation implies a reduction in the probability and/or impact of an adverse risk event to be within acceptable threshold limits. Taking early actions to reduce the probability and/or impact of a risk occurring on the project is often more effective than trying to repair the damage after the risk has occurred.
Answer: B is incorrect. Avoidance changes the project plan to avoid the risk altogether. Answer: C is incorrect. Transference requires shifting some or all of the negative impacts of a threat, along with the ownership of the response, to a third party. Transferring the risk simply gives another party the responsibility for its management-it does not eliminate it. Transferring the liability for a risk is most effective in dealing with financial risk exposure. Risk transference nearly always involves payment of a risk premium to the party taking on the risk.
Answer: D is incorrect. Enhancing is actually a positive risk response. This strategy is used to increase the probability and/or the positive impact of an opportunity. Identifying and maximizing the key drivers of these positive-impact risks may increase the probability of their occurrence.

QUESTION 227
Which of the following processes addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget?

A. Monitor and Control Risk
B. Plan risk response
C. Identify Risks
D. Qualitative Risk Analysis

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The plan risk response project management process aims to reduce the threats to the project objectives and to increase opportunities. It follows the perform qualitative risk analysis process and perform quantitative risk analysis process. Plan risk response process includes the risk response owner to take the job for each agreed-to and funded risk response. This process addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget. The inputs to the plan risk response process are as follows:
Risk register
Risk management plan
Answer: C is incorrect. Identify Risks is the process of determining which risks may affect the project. It also documents risks' characteristics. The Identify Risks process is part of the Project Risk Management knowledge area. As new risks may evolve or become known as the project progresses through its life cycle, Identify Risks is an iterative process. The process should involve the project team so that they can develop and maintain a sense of ownership and responsibility for the risks and associated risk response actions. Risk Register is the only output of this process.
Answer: A is incorrect. Monitor and Control Risk is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying

new risks, and evaluating risk process effectiveness throughout the project. It can involve choosing alternative strategies, executing a contingency or fallback plan, taking corrective action, and modifying the project management plan.
Answer: D is incorrect. Qualitative analysis is the definition of risk factors in terms of high/medium/low or a numeric scale (1 to 10). Hence it determines the nature of risk on a relative scale.
Some of the qualitative methods of risk analysis are:
Scenario analysis- This is a forward-looking process that can reflect risk for a given point in time.
Risk Control Self -assessment (RCSA) - RCSA is used by enterprises (like banks) for the identification and evaluation of operational risk exposure. It is a logical first step and assumes that business owners and managers are closest to the issues and have the most expertise as to the source of the risk. RCSA is a constructive process in compelling business owners to contemplate, and then explain, the issues at hand with the added benefit of increasing their accountability.

QUESTION 228
Out of several risk responses, which of the following risk responses is used for negative risk events?

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

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Among the given choices only Acceptance response is used for negative risk events. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs. If an enterprise adopts a risk acceptance, it should carefully consider who can accept the risk. Risk should be accepted only by senior management in relationship with senior management and the board. There are two alternatives to the acceptance strategy, passive and active.
Passive acceptance means that enterprise has made no plan to avoid or mitigate the risk but willing to accept the consequences of the risk.
Active acceptance is the second strategy and might include developing contingency plans and reserves to deal with risks.
Answer: C, A, and B are incorrect. These all are used to deal with opportunities or positive risks, and not with negative risks.

QUESTION 229
Which of the following is the MOST critical security consideration when an enterprise outsource its major part of IT department to a third party whose servers are in foreign company?

A. A security breach notification may get delayed due to time difference
B. The enterprise could not be able to monitor the compliance with its internal security and privacy guidelines
C. Laws and regulations of the country of origin may not be enforceable in foreign country
D. Additional network intrusion detection sensors should be installed, resulting in additional cost

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Laws and regulations of the country of origin may not be enforceable in foreign country and conversely, it is also true that laws and regulations of the foreign outsourcer may also impact the enterprise. Hence violation of applicable laws may not be recognized or rectified due to lack of knowledge of the local laws.
Answer: B is incorrect. Outsourcing does not remove the enterprise's responsibility regarding internal requirements. Hence monitoring the compliance with its internal security and privacy guidelines is not a problem.
Answer: A is incorrect. Security breach notification is not a problem and also time difference does not play any role in 24/7 environment. Pagers, cellular phones, telephones, etc. are there to communicate the notifications.
Answer: D is incorrect. The need for additional network intrusion detection sensors is not a major problem as it can be easily managed. It only requires addition funding, but can be addressed.

QUESTION 230
You are the Risk Official in Bluewell Inc. You have detected much vulnerability during risk assessment process. What you should do next?

A. Prioritize vulnerabilities for remediation solely based on impact.
B. Handle vulnerabilities as a risk, even though there is no threat.
C. Analyze the effectiveness of control on the vulnerabilities' basis.
D. Evaluate vulnerabilities for threat, impact, and cost of mitigation.

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Vulnerabilities detected during assessment should be first evaluated for threat, impact and cost of mitigation. It should be evaluated and prioritized on the basis whether they impose credible threat or not.
Answer: A and C are incorrect. These are the further steps that are taken after evaluating vulnerabilities. So, these are not immediate action after detecting vulnerabilities. Answer: B is incorrect. If detected vulnerabilities impose no/negligible threat on an enterprise then it is not cost effective to address it as risk.

QUESTION 231
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. Qualitative Risk Analysis
B. Plan Risk Management

C. Identify Risks

D. Quantitative Risk Analysis

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
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: D 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: C 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: B 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 232
You and your project team have identified a few risk events in the project and recorded the events in the risk register. Part of the recording of the events includes the identification of a risk owner. Who is a risk owner?

A. A risk owner is the party that will monitor the risk events.

B. A risk owner is the party that will pay for the cost of the risk event if it becomes an issue.

C. A risk owner is the party that has caused the risk event.

D. A risk owner is the party authorized to respond to the risk event.

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk owner for each risk should be the person who has the most influence over its outcome. Selecting the risk owner thus usually involves considering the source

of risk and identifying the person who is best placed to understand and implement what needs to be done. They are also responsible for responding to the event and reporting on the risk status. Answer: C is incorrect. Risk owners are not the people who cause the risk event. Answer: A is incorrect. A risk owner will monitor the identified risks for status changes, but all project stakeholders should be iteratively looking to identify the risks. Answer: B is incorrect. Risk owners do not pay for the cost of the risk event.

QUESTION 233
Suppose you are working in Company Inc. and you are using risk scenarios for estimating the likelihood and impact of the significant risks on this organization. Which of the following assessment are you doing?

A. IT security assessment
B. IT audit
C. Threat and vulnerability assessment
D. Risk assessment

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Threat and vulnerability assessment consider the full spectrum of risks. It identifies the likelihood of occurrence of risks and impact of the significant risks on the organization using the risk scenarios. For example: Natural threats can be evaluated by using historical data concerning frequency of occurrence for given natural disasters such as tornadoes, hurricanes, floods, fire, etc.
Answer: D is incorrect. Risk assessment uses quantitative and qualitative analysis approaches to evaluate each significant risk identified.
Answer: A and B are incorrect. These use either some technical evaluation tool or assessment methodologies to evaluate risk but do not use risk scenarios.

QUESTION 234
You are the project manager of the PFO project. You are working with your project team members and two subject matter experts to assess the identified risk events in the project. Which of the following approaches is the best to assess the risk events in the project?

A. Interviews or meetings
B. Determination of the true cost of the risk event
C. Probability and Impact Matrix
D. Root cause analysis

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:

Explanation:
Risk probability and assessment is completed through interviews and meetings with the participants that are most familiar with the risk events, the project work, or have other information that can help determine the affect of the risk. Answer: C is incorrect. The probability and impact matrix is a tool and technique to prioritize the risk events, but it's not the best answer for assessing risk events within the project. Answer: B is incorrect. The true cost of the risk event is not a qualitative risk assessment approach. It is often done during the quantitative risk analysis process. Answer: D is incorrect. Root cause analysis is a risk identification technique, not a qualitative assessment tool.

QUESTION 235
Which of the following is BEST described by the definition below?

"They are heavy influencers of the likelihood and impact of risk scenarios and should be taken into account during every risk analysis, when likelihood and impact are assessed."

A. Obscure risk
B. Risk factors
C. Risk analysis
D. Risk event

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk factors are those features that influence the likelihood and/or business impact of risk scenarios. They have heavy influences on probability and impact of risk scenarios. They should be taken into account during every risk analysis, when likelihood and impact are assessed.
Answer: C is incorrect. A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats. A risk from an organizational perspective consists of:
Threats to various processes of organization.
Threats to physical and information assets.
Likelihood and frequency of occurrence from threat.
Impact on assets from threat and vulnerability.
Risk analysis allows the auditor to do the following tasks:
Identify threats and vulnerabilities to the enterprise and its information system. Provide information for evaluation of controls in audit planning.
Aids in determining audit objectives.
Supporting decision based on risks.
Answer: A is incorrect. The enterprise must consider risk that has not yet occurred and should develop scenarios around unlikely, obscure or non-historical events.
Such scenarios can be developed by considering two things:
Visibility
Recognition
For the fulfillment of this task enterprise must:

Be in a position that it can observe anything going wrong Have the capability to recognize an observed event as something wrong Answer: D is incorrect. A risk event represents the situation where you have a risk that only occurs with a certain probability and where the risk itself is represented by a specified distribution.

QUESTION 236
Which of the following processes is described in the statement below? "It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

A. Perform Quantitative Risk Analysis
B. Monitor and Control Risks
C. Identify Risks
D. Perform Qualitative Risk Analysis

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Monitor and Control Risk is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project. It can involve choosing alternative strategies, executing a contingency or fallback plan, taking corrective action, and modifying the project management plan.
Answer: D is incorrect. This is the process of prioritizing risks for further analysis or action by accessing and combining their probability of occurrence and impact.
Answer: C is incorrect. This is the process of determining which risks may affect the project and documenting their characteristics.
Answer: B is incorrect. This is the process of numerically analyzing the effect of identified risks on overall project objectives.

QUESTION 237
You work as a Project Manager for Company Inc. You have to conduct the risk management activities for a project. Which of the following inputs will you use in the plan risk management process?
Each correct answer represents a complete solution. Choose all that apply.

A. Quality management plan
B. Schedule management plan
C. Cost management plan
D. Project scope statement

Correct Answer: BCD
Section: Volume C
Explanation

Explanation/Reference:

Explanation:
The inputs to the plan risk management process are as follows:
Project scope statement: It provides a clear sense of the range of possibilities associated with the project and establishes the framework for how significant the risk management effort may become.
Cost management plan: It describes how risk budgets, contingencies, and management reserves will be reported and accessed.
Schedule management plan: It describes how the schedule contingencies will be reported and assessed.
Communication management plan: It describes the interactions, which occurs on the project and determines who will be available to share information on various risks and responses at different times.
Enterprise environmental factors: It include, but are not limited to, risk attitudes and tolerances that describe the degree of risk that an organization withstand.
Organizational process assets: It includes, but are not limited to, risk categories, risk statement formats, standard templates, roles and responsibilities, authority levels for decision- making, lessons learned, and stakeholder registers. Answer: A is incorrect. It is not an input for Plan risk management process.

QUESTION 238
Which of the following documents is described in the statement below? "It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."

A. Quality management plan
B. Risk management plan
C. Risk register
D. Project charter

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Risk register is a document that contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning. Risk register is developed along with all processes of the risk management from Plan Risk Management through Monitor and Control Risks.
Answer: A is incorrect. The quality management plan is a component of the project management plan. It describes how the project team will implement the organization's quality policy. The quality management plan addresses quality control (QC), quality assurance (QA), and continuous process improvement for the project. Based on the requirement of the project, the quality management plan may be formal or informal, highly detailed or broadly framed. Answer: B is incorrect. Risk management plan includes roles and responsibilities, risk analysis definitions, timing for reviews, and risk threshold. The Plan Risk Responses process takes input from risk management plan and risk register to define the risk response. Answer: D is incorrect. The project charter is the document that formally authorizes a project. The project charter provides the project manager with the authority to apply organizational resources to project activities.

QUESTION 239
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

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
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 240
Which of the following control is used to ensure that users have the rights and permissions they need to perform their jobs, and no more?

A. System and Communications protection control
B. Audit and Accountability control
C. Access control
D. Identification and Authentication control

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Access control 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. Answer: B is incorrect. Audit and Accountability control 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.
Answer: D is incorrect. Identification and Authentication control cover different practices to identify and authenticate users. Each user should be uniquely identified. In other words, each user has one account. This account is only used by one user. Similarly, device identifiers uniquely identify devices on the network.
Answer: A is incorrect. System and Communications protection control is a large group of controls that cover many aspects of protecting systems and communication channels. Denial of service protection and boundary protection controls are included. Transmission integrity and confidentiality controls are also included.

QUESTION 241

You are working in an enterprise. Your enterprise owned various risks. Which among the following is MOST likely to own the risk to an information system that supports a critical business process?

A. System users
B. Senior management
C. IT director
D. Risk management department

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Senior management is responsible for the acceptance and mitigation of all risk. Hence they will also own the risk to an information system that supports a critical business process. Answer: C is incorrect. The IT director manages the IT systems on behalf of the business owners.
Answer: D is incorrect. The risk management department determines and reports on level of risk, but does not own the risk. Risk is owned by senior management.
Answer: A is incorrect. The system users are responsible for utilizing the system properly and following procedures, but they do not own the risk.

QUESTION 242
Which of the following components ensures that risks are examined for all new proposed change requests in the change control system?

A. Configuration management
B. Scope change control
C. Risk monitoring and control
D. Integrated change control

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Integrated change control is the component that is responsible for reviewing all aspects of a change's impact on a project - including risks that may be introduced by the new change. Integrated change control is a way to manage the changes incurred during a project. It is a method that manages reviewing the suggestions for changes and utilizing the tools and techniques to evaluate whether the change should be approved or rejected. Integrated change control is a primary component of the project's change control system that examines the affect of a proposed change on the entire project.
Answer: A is incorrect. Configuration management controls and documents changes to the features and functions of the product scope.
Answer: B is incorrect. Scope change control focuses on the processes to allow changes to enter the project scope.
Answer: C is incorrect. Risk monitoring and control is not part of the change control system, so this choice is not valid.

QUESTION 243
Which of the following are true for threats?
Each correct answer represents a complete solution. Choose three.

A. They can become more imminent as time goes by, or it can diminish
B. They can result in risks from external sources
C. They are possibility
D. They are real
E. They will arise and stay in place until they are properly dealt.

Correct Answer: ABD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Threat is an act of coercion wherein an act is proposed to elicit a negative response. Threats are real, while the vulnerabilities are a possibility. They can result in risks from external sources, and can become imminent by time or can diminish. Answer: C and E are incorrect. These two are true for vulnerability, but not threat. Unlike the threat, vulnerabilities are possibility and can result in risks from internal sources. They will arise and stay in place until they are properly dealt.

QUESTION 244
Which of the following statements BEST describes policy?

A. A minimum threshold of information security controls that must be implemented
B. A checklist of steps that must be completed to ensure information security
C. An overall statement of information security scope and direction
D. A technology-dependent statement of best practices

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
A policy is an executive mandate which helps in identifying a topic that contains particular risks to avoid or prevent. Policies are high-level documents signed by a person of high authority with the power to force cooperation. The policy is a simple document stating that a particular high-level control objective is important to the organization's success. Policies are usually only one page in length. The authority of the person mandating a policy will determine the scope of implementation. Hence in other words, policy is an overall statement of information security scope and direction.

Answer: C, A, and D are incorrect. These are not the valid definitions of the policy.

QUESTION 245
You are the project manager of GHT project. You have analyzed the risk and applied appropriate controls. In turn, you got residual risk as a result of this. Residual risk can be used to determine which of the following?

A. Status of enterprise's risk
B. Appropriate controls to be applied next
C. The area that requires more control
D. Whether the benefits of such controls outweigh the costs

Correct Answer: CD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Residual risk can be used by management to determine:
Which areas require more control Whether the benefits of such controls outweigh the costs As residual risk is the output that comes after applying appropriate controls, so it can also estimate the area which need more sophisticated control. If the cost of control is large that its benefits then no control is applied, hence residual risk can determine benefits of these controls over cost.
Answer: B is incorrect. Appropriate control can only be determined as the result of risk assessment, not through residual risk.
Answer: A is incorrect. Status of enterprise's risk can be determined only after risk monitoring.

QUESTION 246
When it appears that a project risk is going to happen, what is this term called?

A. Issue
B. Contingency response
C. Trigger
D. Threshold

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
A trigger is a warning sign or a condition that a risk event is likely to occur within the project. Answer: B is incorrect. A contingency response is a pre-planned response for a risk event, such as a rollback plan.

Answer: A is incorrect. Issues are events that come about as a result of risk events. Risks become issues only after they have actually occurred. Answer: D is incorrect. A threshold is a limit that the risk passes to actually become an issue in the project.

QUESTION 247
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. Project scope statement
B. Cost management plan
C. Risk register
D. Organizational process assets

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
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: B is incorrect. The cost management plan is the input to the perform quantitative risk analysis process.

QUESTION 248
Which of the following will significantly affect the standard information security governance model?

A. Currency with changing legislative requirements
B. Number of employees
C. Complexity of the organizational structure
D. Cultural differences between physical locations

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Complexity of the organizational structure will have the most significant impact on the Information security governance model. Some of the elements that impact

organizational structure are multiple business units and functions across the organization. Answer: A is incorrect. Currency with changing legislative requirements should not have major impact once good governance models are placed, hence, governance will help in effective management of the organization's ongoing compliance. Answer: B and D are incorrect. The numbers of employees and the distance between physical locations have less impact on
Information security models as well-defined process, technology and people components together provide the proper governance.

QUESTION 249
You are the risk professional in Bluewell Inc. You have identified a risk and want to implement a specific risk mitigation activity. What you should PRIMARILY utilize?

A. Vulnerability assessment report
B. Business case
C. Technical evaluation report
D. Budgetary requirements

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
As business case includes business need (like new product, change in process, compliance need, etc.) and the requirements of the enterprise (new technology, cost, etc.), risk professional should utilize this for implementing specific risk mitigation activity. Risk professional must look at the costs of the various controls and compare them against the benefits that the organization will receive from the risk response. Hence he/she needs to have knowledge of business case development to illustrate the costs and benefits of the risk response. Answer: C, A, and D are incorrect. These all options are supplemental.

QUESTION 250
You are the project manager of the AFD project for your company. You are working with the project team to reassess existing risk events and to identify risk events that have not happened and whose relevancy to the project has passed. What should you do with these events that have not happened and would not happen now in the project?

A. Add the risk to the issues log
B. Close the outdated risks
C. Add the risks to the risk register
D. Add the risks to a low-priority watch-list

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:

Explanation:
Risks that are now outdated should be closed by the project manager, there is no need to keep record of that.
Answer: D is incorrect. Risks with low probability and low impact go on the risk watchlist. Answer: C is incorrect. Identified risks are already in the risk register.
Answer: A is incorrect. Risks do not go into the issue log, but the risk register.

QUESTION 251
What activity should be done for effective post-implementation reviews during the project?

A. Establish the business measurements up front
B. Allow a sufficient number of business cycles to be executed in the new system
C. Identify the information collected during each stage of the project
D. Identify the information to be reviewed

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
For effective post-implementation review the business measurements up front is established during the project.
Answer: D and C are incorrect. Identifying the information to be reviewed and information collected during each stage of project is done in pre-project phase and not during project for effective post-implementation review.
Answer: B is incorrect. Executing sufficient number of business cycles in the new system is done after the completion of the project.

QUESTION 252
Which of the following is the best reason for performing risk assessment?

A. To determine the present state of risk
B. To analyze the effect on the business
C. To satisfy regulatory requirements
D. To budget appropriately for the application of various controls

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
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.

Hence risk assessment helps in determining the present state of the risk.
Answer: D is incorrect. Budgeting appropriately is one the results of risk assessment but is not the reason for performing the risk assessment.
Answer: B is incorrect. Analyzing the effect of risk on an enterprise is the part of the process while performing risk assessment, but is not the reason for doing it.
Answer: C is incorrect. Performing risk assessment may satisfy the regulatory requirements, but is not the reason to perform risk assessment.

QUESTION 253
You are the project manager of GHT project. You identified a risk of noncompliance with regulations due to missing of a number of relatively simple procedures. The response requires creating the missing procedures and implementing them. In which of the following risk response prioritization should this case be categorized?

A. Business case to be made
B. Quick win
C. Risk avoidance
D. Deferrals

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
This is categorized as a "quick win" because the allocation of existing resources or a minor resource investment provides measurable benefits. Quick win is very effective and efficient response that addresses medium to high risk.
Answer: A is incorrect. "Business case to be made" requires careful analysis and management decisions on investments that are more expensive or difficult risk responses to medium to high risk. Here in this scenario, there is only minor investment that is why, it is not "business case to be made".
Answer: D is incorrect. Deferral addresses costly risk response to a low risk, and hence in this specified scenario it is not used.
Answer: C is incorrect. Risk avoidance is a type of risk response and not risk response prioritization option.

QUESTION 254
What are the PRIMARY objectives of a control?

A. Detect, recover, and attack
B. Prevent, respond, and log
C. Prevent, control, and attack
D. Prevent, recover, and detect

Correct Answer: D
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Controls are the policies, procedures, practices and guidelines designed to provide appropriate assurance that business objectives are achieved and undesired events are detected, prevented, and corrected. Controls, or countermeasures, will reduce or neutralize threats or vulnerabilities.
Controls have three primary objectives:
Prevent
Recover
Detect
Answer: C, B, and A are incorrect. One or more objectives stated in these choices is not correct objective of control.

QUESTION 255
You work as the project manager for Company Inc. The project on which you are working 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. Communications Management Plan
C. Risk Management Plan
D. Stakeholder management strategy

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
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: D is incorrect. The stakeholder management strategy does not address risk communications.
Answer: C is incorrect. The Risk Management Plan deals with risk identification, analysis, response, and monitoring.
Answer: A is incorrect. The Resource Management Plan does not define risk communications.

QUESTION 256
You are the project manager of GHT project. You and your team have developed risk responses for those risks with the highest threat to or best opportunity for the project objectives. What are the immediate steps you should follow, after planning for risk response process? Each correct answer represents a complete solution. Choose three.

A. Updating Project management plan and Project document

B. Applying controls
C. Updating Risk register
D. Prepare Risk-related contracts

Correct Answer: ACD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The risk register is updated at the end of the plan risk response process with the information that was discovered during the process. The response plans are recorded in the risk register. Project management plan consisting of WBS, schedule baseline and cost performance baseline should be updated. After planning risk response process, there may be requirement of updating project documents like technical documentation and assumptions, documented in the project scope statement.
If risk response strategies include responses such as transference or sharing, it may be necessary to purchase services or items from third parties. Contracts for those services can be prepared and discussed with the appropriate parties. Answer: B is incorrect. Controls are implemented in the latter stage of risk response process. It is not immediate task after the planning of risk response process, as updating of several documents is done first.
The purpose of the Plan Risk Responses process is to develop risk responses for those risks with the highest threat to or best opportunity for the project objectives. The Plan Risk Responses process has four outputs:
Risk register updates
Risk-related contract decisions
Project management plan updates
Project document updates

QUESTION 257
Which of the following assets are the examples of intangible assets of an enterprise? Each correct answer represents a complete solution. Choose two.

A. Customer trust
B. Information
C. People
D. Infrastructure

Correct Answer: AB
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
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.

QUESTION 258
You are the project manager of the GHY project for your company. This project has a budget of $543,000 and is expected to last 18 months. In this project, you have identified several risk events and created risk response plans. In what project management process group will you implement risk response plans?

A. Monitoring and Controlling
B. In any process group where the risk event resides
C. Planning
D. Executing

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The monitor and control project risk process resides in the monitoring and controlling project management process group. This process is responsible for implementing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness through the project.
Answer: C is incorrect. Risk response plans are not implemented as part of project planning. Answer: D is incorrect. Risk response plans are not implemented as part of project execution. Answer: B is incorrect. Risk response plans are implemented as part of the monitoring and controlling process group.

QUESTION 259
During which of the following processes, probability and impact matrix are prepared?

A. Risk response
B. Monitoring and Control Risk
C. Quantitative risk assessment
D. Qualitative risk assessment

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The probability and impact matrix is a technique to prioritize identified risks of the project on their risk rating, and are being prepared while performing qualitative

risk analysis. Evaluation of each risk's importance and, hence, priority for attention, is typically conducted using a look-up table or a probability and impact matrix. This matrix specifies combinations of probability and impact that lead to rating the risks as low, moderate, or high priority. Answer: C is incorrect. SLE, ARO and ALE are used in quantitative risk assessment. Answer: A and B are incorrect. These processes are part of Risk Management. The probability and impact matrix is prepared during the qualitative risk analysis for further quantitative analysis and response based on their risk rating.

QUESTION 260

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. Enhance

B. Exploit

C. Accept

D. Share

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:

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

QUESTION 261

Your project has several risks that may cause serious financial impact if they occur. You have studied the risk events and made some potential risk responses for the risk events but management wants you to do more. They'd like you to create some type of a chart that identified the risk probability and impact with a financial amount for each risk event. What is the likely outcome of creating this type of chart?

A. Risk response plan

B. Contingency reserve

C. Risk response

D. Quantitative analysis

Correct Answer: B
Section: Volume D

Explanation

Explanation/Reference:
Explanation:
This chart is a probability-impact matrix in a quantitative analysis process. The probability and financial impact of each risk is learned through research, testing, and subject matter experts. The probability of the event is multiplied by the financial impact to create a risk event value for each risk. The sum of the risk event values will lead to the contingency reserve for the project.
Answer: C is incorrect. The risk responses are needed but this chart doesn't help the project manager to create them.
Answer: A is incorrect. The risk response plan is based on the risk responses, not the risk probability-impact matrix.
Answer: D is incorrect. This chart is created as part of quantitative analysis.

QUESTION 262
Which of the following are parts of SWOT Analysis?
Each correct answer represents a complete solution. Choose all that apply.

A. Weaknesses
B. Tools
C. Threats
D. Opportunities
E. Strengths

Correct Answer: ACDE
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
SWOT analysis is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats involved in a project or in a business venture. It involves specifying the objective of the business venture or project and identifying the internal and external factors that are favorable and unfavorable to achieving that objective. The technique is credited to Albert Humphrey, who led a research project at Stanford University in the 1960s and 1970s using data from Fortune 500 companies. Answer: B is incorrect. Tools are not the parts of SWOT analysis.

QUESTION 263
What is the FIRST phase of IS monitoring and maintenance process?

A. Report result
B. Prioritizing risks
C. Implement monitoring
D. Identifying controls

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Following are the phases that are involved in Information system monitoring and maintenance:
Following are the phases that are involved in Information system monitoring and maintenance:
Prioritize risk: The first phase involves the prioritization of risk which in turn involves following task:
Analyze and prioritize risks to organizational objectives. Identify the necessary application components and flow of information through the system. Examine and understand the functionality of the application by reviewing the application system documentation and interviewing appropriate personnel. Identify controls: After prioritizing risk now the controls are identified, and this involves following tasks:
Key controls are identified across the internal control system that addresses the prioritized risk.
Applications control strength is identified.
Impact of the control weaknesses is being evaluated. Testing strategy is developed by analyzing the accumulated information. Identify information: Now the IS control information should be identified:
Identify information that will persuasively indicate the operating effectiveness of the internal control system.
Observe and test user performing procedures .
Implement monitoring: Develop and implement cost-effective procedures to evaluate the persuasive information.
Report results: After implementing monitoring process the results are being reported to relevant stakeholders.
Answer: D, A, and C are incorrect. These all phases occur in IS monitoring and maintenance process after prioritizing risks.

QUESTION 264
You are the project manager for the NHH project. You are working with your project team to examine the project from four different defined perspectives to increase the breadth of identified risks by including internally generated risks. What risk identification approach are you using in this example?

A. Root cause analysis
B. Influence diagramming techniques
C. SWOT analysis
D. Assumptions analysis

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
This is an example of SWOT analysis. SWOT analysis examines the strengths, weaknesses, opportunities, and threats within the project and generated from within the organization. SWOT stands for Strengths, Weaknesses, Opportunities, and Threats. It is a part of business policy that helps an individual or a company to make decisions. It includes the strategies to build the strength of a company and use the opportunities to make the company successful. It also includes the strategies to overcome the weaknesses of and threats to the company. Answer: D is incorrect. Assumptions analysis does not use four pre-defined perspectives

for review.
Answer: A is incorrect. Root cause analysis examines causal factors for events within the project.
Answer: B is incorrect. Influence diagramming techniques examines the relationships between things and events within the project.

QUESTION 265
You are working in an enterprise. Assuming that your enterprise periodically compares finished goods inventory levels to the perpetual inventories in its ERP system. What kind of information is being provided by the lack of any significant differences between perpetual levels and actual levels?

A. Direct information
B. Indirect information
C. Risk management plan
D. Risk audit information

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The lack of any significant differences between perpetual levels and actual levels provides indirect information that its billing controls are operating. It does not provide any direct information.
Answer A is incorrect. It does not provide direct information as there is no information about the propriety of cutoff.
Answer: D and C are incorrect. These are not the types of information.

QUESTION 266
In which of the following risk management capability maturity levels does the enterprise takes major business decisions considering the probability of loss and the probability of reward? Each correct answer represents a complete solution. Choose two.

A. Level 0
B. Level 2
C. Level 5
D. Level 4

Correct Answer: CD
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Enterprise having risk management capability maturity level 4 and 5 takes business decisions considering the probability of loss and the probability of reward, i.e.,

considering all the aspects of risk.
Answer: A is incorrect. Enterprise having risk management capability maturity level 0 takes business decisions without considering risk credential information.
Answer: B is incorrect. At this low level of risk management capability the enterprise take decisions considering specific risk issues within functional and business silos (e.g., security, business continuity, operations).

QUESTION 267
Henry is the project sponsor of the JQ Project and Nancy is the project manager. Henry has asked Nancy to start the risk identification process for the project, but Nancy insists that the project team be involved in the process. Why should the project team be involved in the risk identification?

A. So that the project team can develop a sense of ownership for the risks and associated risk responsibilities.
B. So that the project manager can identify the risk owners for the risks within the project and the needed risk responses.
C. So that the project manager isn't the only person identifying the risk events within the project.
D. So that the project team and the project manager can work together to assign risk ownership.

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The best answer to include the project team members is that they'll need to develop a sense of ownership for the risks and associated risk responsibilities. Answer: C is incorrect. While the project manager shouldn't be the only person to identify the risk events, this isn't the best answer.
Answer: D is incorrect. The reason to include the project team is that the project team needs to develop a sense of ownership for the risks and associated risk responsibilities, not to assign risk ownership.
Answer: B is incorrect. The reason to include the project team is that the project team needs to develop a sense of ownership for the risks and associated risk responsibilities, not to assign risk ownership and risk responses at this point.

QUESTION 268
Which of the following establishes mandatory rules, specifications and metrics used to measure compliance against quality, value, etc?

A. Framework
B. Legal requirements
C. Standard
D. Practices

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:

Explanation:
Standard establishes mandatory rules, specifications and metrics used to measure compliance against quality, value, etc. Standards are usually intended for compliance purposes and to provide assurance to others who interact with a process or outputs of a process. Answer: A is incorrect. Frameworks are generally accepted, business-process-oriented structures that establish a common language and enable repeatable business processes. Answer: D is incorrect. Practices are frequent or usual actions performed as an application of knowledge. A leading practice would be defined as an action that optimally applies knowledge in a particular area. They are issued by a "recognized authority" that is appropriate to the subject matter. issuing bodies may include professional associations and academic institutions or commercial entities such as software vendors. They are generally based on a combination of research, expert insight and peer review. Answer: B is incorrect. These are legal rules underneath which project has to be.

QUESTION 269
You are the project manager of your enterprise. While performing risk management, you are given a task to identify where your enterprise stand in certain practice and also to suggest the priorities for improvements. Which of the following models would you use to accomplish this task?

A. Capability maturity model
B. Decision tree model
C. Fishbone model
D. Simulation tree model

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Capability maturity models are the models that are used by the enterprise to rate itself in terms of the least mature level (having nonexistent or unstructured processes) to the most mature (having adopted and optimized the use of good practices). The levels within a capability maturity model are designed to allow an enterprise to identify descriptions of its current and possible future states. In general, the purpose is to:
Identify, where enterprises are in relation to certain activities or practices.
Suggest how to set priorities for improvements
Answer: D is incorrect. There is no such model exists in risk management process. Answer: B is incorrect. 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.
Answer: C is incorrect. Fishbone diagrams or Ishikawa diagrams shows the relationships between the causes and effects of problems.

QUESTION 270
You are the risk official in Techmart Inc. You are asked to perform risk assessment on the impact of losing a server. For this assessment you need to calculate monetary value of the server. On which of the following bases do you calculate monetary value?

A. Cost to obtain replacement
B. Original cost to acquire
C. Annual loss expectancy
D. Cost of software stored

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The monetary value of the server should be based on the cost of its replacement. However, the financial impact to the enterprise may be much broader, based on the function that the server performs for the business and the value it brings to the enterprise. Answer: C, D, and B are incorrect. Cost of software is not been counted because it can be restored from the back-up media. On the other hand' Ale for all risk related to the server does not represent the server's value. Lastly, the original cost may be significantly different from the current cost and, therefore, not relevant to this.

QUESTION 271
Which of the following is the BEST way of managing risk inherent to wireless network?

A. Enabling auditing on every host that connects to a wireless network
B. Require private, key-based encryption to connect to the wireless network
C. Require that the every host that connect to this network have a well-tested recovery plan
D. Enable auditing on every connection to the wireless network

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
As preventive control and prevention is preferred over detection and recovery, therefore, private and key-based encryption should be adopted for managing risks. Answer: A, C, and D are incorrect. As explained in above section preventive control and prevention is preferred over detection and recovery, hence these are less preferred way.

QUESTION 272
You are elected as the project manager of GHT project. You have to initiate the project. Your Project request document has been approved, and now you have to start working on the project. What is the FIRST step you should take to initialize the project?

A. Conduct a feasibility study

B. Acquire software
C. Define requirements of project
D. Plan project management

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Conducting a feasibility study begins once initial approval has been given to move forward with a project. It includes an analysis to clearly define the need and to identify alternatives for addressing the need.
Answer: B is incorrect. Acquiring software involves building new or modifying existing hardware or software after final approval by the stakeholder, which is not a phase in the standard SDLC process.
If a decision was reached to acquire rather than develop software, this task should occur after feasibility study and defining requirements.
Answer: D is incorrect. This is latter phase in project development process. Answer: C is incorrect. Requirements of the project is being defined after conducting feasibility study.

QUESTION 273
John is the project manager of the NHQ Project for his company. His project has 75 stakeholders, some of which are external to the organization. John needs to make certain that he communicates about risk in the most appropriate method for the external stakeholders. Which project management plan will be the best guide for John to communicate to the external stakeholders?

A. Risk Response Plan
B. Communications Management Plan
C. Project Management Plan
D. Risk Management Plan

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The Communications Management Plan will direct John on the information to be communicated, when to communicate, and how to communicate with external stakeholders. 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: D is incorrect. The Risk Management Plan defines how risks will be identified, analyzed, responded to, and controlled throughout the project. Answer: A is

incorrect. The Risk Response Plan identifies how risks will be responded to. Answer: C is incorrect. The Project Management Plan is the parent of all subsidiary management plans and it is not the most accurate choice for this

QUESTION 274
Adrian is a project manager for a new project using a technology that has recently been released and there's relatively little information about the technology. Initial testing of the technology makes the use of it look promising, but there's still uncertainty as to the longevity and reliability of the technology. Adrian wants to consider the technology factors a risk for her project. Where should she document the risks associated with this technology so she can track the risk status and responses?

A. Project scope statement
B. Project charter
C. Risk low-level watch list
D. Risk register

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains:
A description of the risk
The impact should this event actually occur
The probability of its occurrence
Risk Score (the multiplication of Probability and Impact) A summary of the planned response should the event occur A summary of the mitigation (the actions taken in advance to reduce the probability and/or impact of the event)
Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved. It records the initial risks, the potential responses, and tracks the status of each identified risk in the project.
Answer: B is incorrect. The project charter does not define risks. Answer: A is incorrect. The project scope statement does document initially defined risks but it is not a place that will record risks responses and status of risks. Answer: C is incorrect. The risk low-level watch list is for identified risks that have low impact and low probability in the project.

QUESTION 275
You are the administrator of your enterprise. Which of the following controls would you use that BEST protects an enterprise from unauthorized individuals gaining access to sensitive information?

A. Monitoring and recording unsuccessful logon attempts
B. Forcing periodic password changes
C. Using a challenge response system
D. Providing access on a need-to-know basis

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Physical or logical system access should be assigned on a need-to-know basis, where there is a legitimate business requirement based on least privilege and segregation of duties. This is done by user authentication.
Answer: C is incorrect. Challenge response system is used to verify the user's identification but does not completely address the issue of access risk if access was not appropriately designed in the first place.
Answer: B is incorrect. Forcing users to change their passwords does not ensure that access control is appropriately assigned.
Answer: A is incorrect. Monitoring and recording unsuccessful logon attempts does not address the risk of appropriate access rights. In other words, it does not prevent unauthorized access.

QUESTION 276
You are the project manager of GHT project. You have identified a risk event on your current project that could save $670,000 in project costs if it occurs. Your organization is considering hiring a vendor to help establish proper project management techniques in order to assure it realizes these savings. Which of the following statements is TRUE for this risk event?

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

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
This risk event has the potential to save money on project costs and organization is hiring a vendor to assure that all these saving are being realized. Hence this risk event involves sharing with a third party to help assure that the opportunity take place. Answer: A is incorrect. This risk event is not accepted as this event has potential to save money as well as it is shared with a vendor so that all these savings are being realized. Answer: C is incorrect. This risk event can be exploited but as here in this scenario, it is stated that organization is hiring vendor, therefore event is being shared not exploited. Answer: B is incorrect. The risk event is mitigated when it has negative impacts. But here it is positive consequences (i.e., saving), therefore it is not mitigated.

QUESTION 277
Which of the following role carriers has to account for collecting data on risk and articulating risk?

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

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
CRO is the individual who oversees all aspects of risk management across the enterprise. Chief risk officer has the main accountability for collecting data and articulating risk. If there is any fault in these processes then CRO should be answerable. Answer: A is incorrect. Enterprise risk committee are the executives who are accountable for the enterprise level collaboration and consensus required to support enterprise risk management (ERM). They are to some extent responsible for articulating risk but are not accounted for it. They are neither responsible nor accounted for collecting data on risk. Answer: C is incorrect. 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 towards collecting data and articulating risk but is not accounted for them.
Answer: B is incorrect. Business process owner is an individual responsible for identifying process requirements, approving process design and managing process performance. He/she is responsible for collecting data and articulating risk but is not accounted for them.

QUESTION 278
Which of the following is NOT true for effective risk communication?

A. Risk information must be known and understood by all stakeholders.
B. Use of technical terms of risk
C. Any communication on risk must be relevant
D. For each risk, critical moments exist between its origination and its potential business consequence

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
For effective communication, information communicated should not inundate the recipients. All ground rules of good communication apply to communication on risk. This includes the avoidance of jargon and technical terms regarding risk because the intended audiences are generally not deeply technologically skilled. Hence use of technical terms is avoided for effective communication Answer: A, C, and D are incorrect. These all are true for effective risk communication. For effective risk communication the risk information should be clear, concise, useful and timely. Risk information must be known and understood by all the stakeholders. Information or communication should not overwhelm the recipients. This includes the avoidance of technical terms regarding risk because the

intended audiences are generally not much technologically skilled.
Any communication on risk must be relevant. Technical information that is too detailed or is sent to inappropriate parties will hinder, rather than enable, a clear view of risk. For each risk, critical moments exist between its origination and its potential business consequence. Information should also be aimed at the correct target audience and available on need-to- know basis.
Hence for effective risk communication risk information should be:
Clear
Concise
Useful
Timely given
Aimed at the correct audience
Available on need-to-know basis

QUESTION 279
Which of the following interpersonal skills has been identified as one of the biggest reasons for project success or failure?

A. Motivation
B. Influencing
C. Communication
D. Political and cultural awareness

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Communication has been identified as one of the biggest reasons for why projects succeeds or fails. Effective communication is essential for good project management. Communication is a process in which information is passed from one person to another. A manager asks his subordinates to accomplish the task assigned to them. He should successfully pass the information to his subordinates. It is a means of motivating and guiding the employees of an enterprise.
Answer: A is incorrect. While motivation is one of the important interpersonal skill, but it is not the best answer.
Answer: B is incorrect. Influencing the project stakeholders is a needed interpersonal skill, but it is not the best answer.
Answer: D is incorrect. Political and cultural awareness is an important part of every project, but it is not the best answer for this

QUESTION 280
You are the project manager of the GHY project for your organization. You are working with your project team to begin identifying risks for the project. As part of your preparation for identifying the risks within the project you will need eleven inputs for the process. Which one of the following is NOT an input to the risk identification process?

A. Quality management plan
B. Stakeholder register

C. Cost management plan

D. Procurement management plan

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The procurement management plan is not one of the eleven inputs for the risk identification process. The eleven inputs to this process are:
risk management plan, activity cost estimates, activity duration estimates, scope baseline, stakeholder register, cost management plan, schedule management plan, quality management plan, project documents, enterprise environmental factors, and organizational process assets.

QUESTION 281
Which of the following come under the phases of risk identification and evaluation? Each correct answer represents a complete solution. Choose three.

A. Maintain a risk profile

B. Collecting data

C. Analyzing risk

D. Applying controls

Correct Answer: ABC
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Risk identification is the process of determining which risks may affect the project. It also documents risks' characteristics.
Following are high-level phases that are involved in risk identification and evaluation:
Collecting data- Involves collecting data on the business environment, types of events, risk categories, risk scenarios, etc., to identify relevant data to enable effective risk identification, analysis and reporting.
Analyzing risk- Involves analyzing risk to develop useful information which is used while taking risk-decisions. Risk-decisions take into account the business relevance of risk factors. Maintain a risk profile- Requires maintaining an up-to-date and complete inventory of known threats and their attributes (e.g., expected likelihood, potential impact, and disposition), IT resources, capabilities, and controls as understood in the context of business products, services and processes to effectively monitor risk over time. Answer: D is incorrect. It comes under risk management process, and not in risk identification and evaluation process.

QUESTION 282
How are the potential choices of risk based decisions are represented in decision tree analysis?

A. End node

B. Root node
C. Event node
D. Decision node

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The potential choices of risk based decisions are represented in decision tree analysis via. Decision node, as decision nodes refers to the available choices. Answer: B is incorrect. Root nodes represent the start of a decision tree. Answer: A is incorrect. End nodes are the final outcomes of the entire decision tree framework, especially in multilayered decision-making situations. Answer: C is incorrect. Event nodes represents the possible uncertain outcomes of the decision, and not the available choices.

QUESTION 283
You are the project manager of the HJK Project for your organization. You and the project team have created risk responses for many of the risk events in the project. Where should you document the proposed responses and the current status of all identified risks?

A. Stakeholder management strategy
B. Lessons learned documentation
C. Risk register
D. Risk management plan

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Risks and the corresponding responses are documented in the risk register for the project. Risk register is a document that contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning. Description, category, cause, probability of occurring, impact on objectives, proposed responses, owner, and the current status of all identified risks are put in the risk register. Answer: B is incorrect. The outcome of risk events and the corresponding risk responses may be documented in the project's lessons learned documented, but the best answer is to document the risk responses as part of the risk register. Answer: D is incorrect. The risk management plan defines how risks will be identified and analyzed, the available responses, and the monitoring and controlling of the risk events. The actual risk responses are included in the risk register. Answer: A is incorrect. The stakeholder management strategy defines how stakeholders and their threats, perceived threats, opinions, and influence over the project objectives will be addressed and managed.

QUESTION 284
Which is the MOST important parameter while selecting appropriate risk response?

A. Cost of response
B. Capability to implement response
C. Importance of risk
D. Efficiency of response

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The cost of the response, which is applied so as to reduce risk within tolerance levels, is one of the most important parameter. By considering the cost of response, it is decided whether or not benefits of applying response is greater than accepting the risk; and according to this analysis it is decided whether the certain response should be applied or not. For example, if risk transfer response is applied by using insurance, then cost would be the cost of insurance. Answer: C is incorrect. This is one of the parameters that is considered but is not as important as considering cost of response. The importance of the risk is determined by the combination of likelihood and magnitude levels along with its position on the risk map. Answer: B is incorrect. This parameter is considered after analyzing the cost of response, which will further decide the level of sophistication of risk response. The enterprise's capability to implement the response means that if the risk management process is mature then the risk response is more Answer: D is incorrect. Efficiency of response can only be analyzed after applying the response. So it is the latter stage in selection of response.

QUESTION 285
You are the project manager of HFD project. You have identified several project risks. You have adopted alternatives to deal with these risks which do not attempt to reduce the probability of a risk event or its impacts. Which of the following response have you implemented?

A. Acceptance
B. Mitigation
C. Avoidance
D. Contingent response

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Contingent response strategy, also known as contingency planning, involves adopting alternatives to deal with the risks in case of their occurrence. Unlike the mitigation planning in which mitigation looks to reduce the probability of the risk and its impact, contingency planning doesn't necessarily attempt to reduce the probability of a risk event or its impacts. Contingency comes into action when the risk event actually occurs. Answer: B is incorrect. Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together. The

main control types are:
Managerial(e.g.,policies)
Technical (e.g., tools such as firewalls and intrusion detection systems) Operational (e.g., procedures, separation of duties) Preparedness activities
Answer: A is incorrect. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs. If an enterprise adopts a risk acceptance, it should carefully consider who can accept the risk. Risk should be accepted only by senior management in relationship with senior management and the board. There are two alternatives to the acceptance strategy, passive and active.
Passive acceptance means that enterprise has made no plan to avoid or mitigate the risk but willing to accept the consequences of the risk.
Active acceptance is the second strategy and might include developing contingency plans and reserves to deal with risks.
Answer: C is incorrect. Risk avoidance means to evade risk altogether, eliminate the cause of the risk event, or change the project plan to protect the project objectives from the risk event.

QUESTION 286
In which of the following risk management capability maturity levels risk appetite and tolerance are applied only during episodic risk assessments?

A. Level 3
B. Level 2
C. Level 4
D. Level 1

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
An enterprise's risk management capability maturity level is 1 when:
There is an understanding that risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk. Any risk identification criteria vary widely across the enterprise. Risk appetite and tolerance are applied only during episodic risk assessments. Enterprise risk policies and standards are incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms. Risk management skills exist on an ad hoc basis, but are not actively developed. Ad hoc inventories of controls that are unrelated to risk are dispersed across desktop applications.
Answer: A is incorrect. In level 3 of risk management capability maturity model, local tolerances drive the enterprise risk tolerance.
Answer: B is incorrect. In level 2 of risk management capability maturity model, risk tolerance is set locally and may be difficult to aggregate. Answer: C is incorrect. In level 4 of risk management capability maturity model, business risk tolerance is reflected by enterprise policies and standards reflect.

QUESTION 287
A project team member has just identified a new project risk. The risk event is determined to have significant impact but a low probability in the project. Should the risk event happen it'll cause the project to be delayed by three weeks, which will cause new risk in the project. What should the project manager do with the risk event?

A. Add the identified risk to a quality control management chart.

B. Add the identified risk to the issues log.
C. Add the identified risk to the risk register.
D. Add the identified risk to the low-level risk watch-list.

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
All identified risks, their characteristics, responses, and their status should be added and monitored as part of the risk register. A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains:
A description of the risk
The impact should this event actually occur
The probability of its occurrence
Risk Score (the multiplication of Probability and Impact) A summary of the planned response should the event occur A summary of the mitigation (the actions taken in advance to reduce the probability and/or impact of the event)
Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved. Answer: D is incorrect. Risks that have a low probability and a low impact may go on the low-level risk watch-list.
Answer: B is incorrect. This is a risk event and should be recorded in the risk register. Answer: A is incorrect. Control management charts are not the place where risk events are recorded.

QUESTION 288
A teaming agreement is an example of what type of risk response?

A. Acceptance
B. Mitigation
C. Transfer
D. Share

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Teaming agreements are often comes under sharing risk response, as they involves joint ventures to realize an opportunity that an organization would not be able to seize otherwise. Sharing response is where two or more entities share a positive risk. Teaming agreements are good example of sharing the reward that comes from the risk of the opportunity. Answer: A is incorrect. Acceptance is a risk response that is appropriate for positive or negative risk events. It does not pursue the

risk, but documents the event and allows the risk to happen. Often acceptance is used for low probability and low impact risk events. Answer: C is incorrect. Transference is a negative risk response where the project manager hires a third party to own the risk event.
Answer: B is incorrect. Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together.

QUESTION 289
You are the project manager of HJT project. Important confidential files of your project are stored on a computer. Keeping the unauthorized access of this computer in mind, you have placed a hidden CCTV in the room, even on having protection password. Which kind of control CCTV is?

A. Technical control
B. Physical control
C. Administrative control
D. Management control

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
CCTV is a physical control.
Physical controls protect the physical environment. They include basics such as locks to protect access to secure areas. They also include environmental controls.
This section presents the following examples of physical controls:
Locked doors, guards, access logs, and closed-circuit television Fire detection and suppression
Temperature and humidity detection
Electrical grounding and circuit breakers
Water detection
Answer: C, A, and D are incorrect. CCTV is a physical control.

QUESTION 290
You are preparing to complete the quantitative risk analysis process with your project team and several subject matter experts. You gather the necessary inputs including the project's cost management plan. Why is it necessary to include the project's cost management plan in the preparation for the quantitative risk analysis process?

A. The project's cost management plan provides control that may help determine the structure for quantitative analysis of the budget.
B. The project's cost management plan can help you to determine what the total cost of the project is allowed to be.
C. The project's cost management plan provides direction on how costs may be changed due to identified risks.
D. The project's cost management plan is not an input to the quantitative risk analysis process.

Correct Answer: A

Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The cost management plan is an input to the quantitative risk analysis process because of the cost management control it provides.
The cost management plan sets how the costs on a project are managed during the project's lifecycle. It defines the format and principles by which the project costs are measured, reported, and controlled. The cost management plan identifies the person responsible for managing costs, those who have the authority to approve changes to the project or its budget, and how cost performance is quantitatively calculated and reported upon. Answer: D is incorrect. This is not a valid statement. The cost management plan is an input to the quantitative risk analysis process.
Answer: B is incorrect. The cost management plan defines the estimating, budgeting, and control of the project's cost.
Answer: C is incorrect. While the cost management plan does define the cost change control system, this is not the best answer for this

QUESTION 291
You are the project manager for BlueWell Inc. Your current project is a high priority and high profile project within your organization. You want to identify the project stakeholders that will have the most power in relation to their interest on your project. This will help you plan for project risks, stakeholder management, and ongoing communication with the key stakeholders in your project. In this process of stakeholder analysis, what type of a grid or model should you create based on these conditions?

A. Stakeholder power/interest grid
B. Stakeholder register
C. Influence/impact grid
D. Salience model

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The power/interest grid groups stakeholders based on their level of authority (power) and their level of interest in your project. The power/interest grid forms a group of the stakeholders based on their level of authority (power) and their level of interest in the project. Interest accounts to what degree the stakeholders are affected by examining the project or policy change, and to what degree of interest or concern they have about it. Power accounts for the influence the stakeholders have over the project or policy, and to what degree they can help to accomplish, or block, the preferred change. Stakeholders, who have high power and interests associated with the project, are the people or organizations that are fully engaged with the project. When trying to generate strategic change, this community is the target of any operation. Answer: B is incorrect. The stakeholder register is a listing of stakeholder information and communication requirements.
Answer: D is incorrect. The salience model groups the stakeholders based on their power, urgency, and legitimacy in the project.
Answer: C is incorrect. The influence/impact grid charts is based on the stakeholders involvement and ability to effect changes to the project's planning and execution.

QUESTION 292

You work as a project manager for BlueWell Inc. You have declined a proposed change request because of the risk associated with the proposed change request. Where should the declined change request be documented and stored?

A. Change request log
B. Project archives
C. Lessons learned
D. Project document updates

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The change request log records the status of all change requests, approved or declined. The change request log is used as an account for change requests and as a means of tracking their disposition on a current basis. The change request log develops a measure of consistency into the change management process. It encourages common inputs into the process and is a common estimation approach for all change requests. As the log is an important component of project requirements, it should be readily available to the project team members responsible for project delivery. It should be maintained in a file with read- only access to those who are not responsible for approving or disapproving project change requests.
Answer: C is incorrect. Lessons learned are not the correct place to document the status of a declined, or approved, change request.
Answer: B is incorrect. The project archive includes all project documentation and is created through the close project or phase process. It is not the best choice for this option D is incorrect. The project document updates is not the best choice for this be fleshed into the project documents, but the declined changes are part of the change request log.

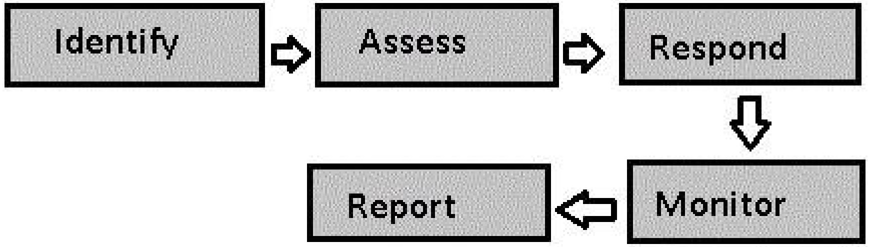
QUESTION 293
Which of the following comes under phases of risk management?

A. Assessing risk
B. Prioritization of risk
C. Identify risk
D. Monitoring risk
E. Developing risk

Correct Answer: ABCD
Section: Volume D
Explanation

Explanation/Reference:
Explanation:

Risk management provides an approach for individuals and groups to make a decision on how to deal with potentially harmful situations.
Following are the four phases involved in risk management:
1.Risk identification :The first thing we must do in risk management is to identify the areas of the project where the risks can occur.
This is termed as risk identification. Listing all the possible risks is proved to be very productive for the enterprise as we can cure them before it can occur. In risk identification both threats and opportunities are considered, as both carry some level of risk with them. 2.Risk Assessment and Evaluation :Risk assessment use quantitative and qualitative analysis approaches to evaluate each significant risk identified. 3.Risk Prioritization and Response :As many risks are being identified in an enterprise, it is best to give each risk a score based on its likelihood and significance in form of ranking. This concludes whether the risk with high likelihood and high significance must be given greater attention as compared to similar risk with low likelihood and low significance. Hence, risks can be prioritized and appropriate responses to those risks are created. 4.Risk Monitoring :Risk monitoring is an activity which oversees the changes in risk assessment. Over time, the likelihood or significance originally attributed to a risk may change. This is especially true when certain responses, such as mitigation, have been made.



QUESTION 294
You are the project manager in your enterprise. You have identified occurrence of risk event in your enterprise. You have pre-planned risk responses. You have monitored the risks that had occurred. What is the immediate step after this monitoring process that has to be followed in response to risk events?

A. Initiate incident response
B. Update the risk register
C. Eliminate the risk completely
D. Communicate lessons learned from risk events

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
When the risk events occur then following tasks have to done to react to it:
Maintain incident response plans
Monitor risk

Initiate incident response
Communicate lessons learned from risk events

QUESTION 295
You are the project manager for GHT project. You need to perform the Qualitative risk analysis process. When you have completed this process, you will produce all of the following as part of the risk register update output except which one?

A. Probability of achieving time and cost estimates
B. Priority list of risks
C. Watch list of low-priority risks
D. Risks grouped by categories

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Probability of achieving time and cost estimates is an update that is produced from the Quantitative risk analysis process. In Qualitative risk analysis probability of occurrence of a specific risk is identified but not of achieving time and cost estimates.

QUESTION 296
You have been assigned as the Project Manager for a new project that involves building of a new roadway between the city airport to a designated point within the city. However, you notice that the transportation permit issuing authority is taking longer than the planned time to issue the permit to begin construction. What would you classify this as?

A. Project Risk
B. Status Update
C. Risk Update
D. Project Issue

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
This is a project issue. It is easy to confuse this as a project risk; however, a project risk is always in the future. In this case, the delay by the permitting agency has already happened; hence this is a project issue. The possible impact of this delay on the project cost, schedule, or performance can be classified as a project risk.
Answer: A is incorrect. It is easy to confuse this as a project risk; however, a project risk is always in the future. In this case, the delay by the permitting agency has

already happened; hence this is a project issue.
Answer: C and B are incorrect as they are extraneous choices and are not applicable.

QUESTION 297
You are the project manager of GHT project. A stakeholder of this project requested a change request in this project. What are your responsibilities as the project manager that you should do in order to approve this change request?
Each correct answer represents a complete solution. Choose two.

A. Archive copies of all change requests in the project file.
B. Evaluate the change request on behalf of the sponsor
C. Judge the impact of each change request on project activities, schedule and budget.
D. Formally accept the updated project plan

Correct Answer: AC
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Project manager responsibilities related to the change request approval process is judging the impact of each change request on project activities, schedule and budget, and also archiving copies of all change requests in the project file.
Answer: B is incorrect. This is the responsibility of Change advisory board. Answer: D is incorrect. Pm has not the authority to formally accept the updated project plan. This is done by project sponsors so as to approve the change request.

QUESTION 298
Natural disaster is BEST associated to which of the following types of risk?

A. Short-term
B. Long-term
C. Discontinuous
D. Large impact

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Natural disaster can be a long-term or short-term and can have large or small impact on the company. However, as the natural disasters are unpredictable and infrequent, they are best considered as discontinuous.

Answer: A is incorrect. Natural disaster can be a short-term, but it is not the best answer. Answer: B is incorrect. Natural disaster can be a long-term, but it is not the best answer. Answer: D is incorrect. Natural disaster can be of large impact depending upon its nature, but it is not the best answer.

QUESTION 299
Which of the following controls focuses on operational efficiency in a functional area sticking to management policies?

A. Internal accounting control
B. Detective control
C. Administrative control
D. Operational control

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Administrative control is one of the objectives of internal control and is concerned with ensuring efficiency and compliance with management policies. Answer: B is incorrect. Detective control simply detects and reports on the occurrence of an error, omission or malicious act.
Answer: A is incorrect. It controls accounting operations, including safeguarding assets and financial records.
Answer: D is incorrect. It focuses on day-to-day operations, functions, and activities. It also ensures that all the organization's objectives are being accomplished.

QUESTION 300
You are the project manager of HJT project. You want to measure the operational effectiveness of risk management capabilities. Which of the following is the BEST option to measure the operational effectiveness?

A. Key risk indicators
B. Capability maturity models
C. Key performance indicators
D. Metric thresholds

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Key performance indicators are a set of quantifiable measures that a company or industry uses to gauge or compare performance in terms of meeting their strategic and operational goals. Key performance indicators (KPIs) provide insights into the operational effectiveness of the concept or capability that they monitor.
Answer: A is incorrect. Key risk Indicators (KRIs) only provide insights into potential risks that may exist or be realized within a concept or capability that they

monitor. Answer: B is incorrect. Capability maturity models (CMMs) assess the maturity of a concept or capability and do not provide insights into operational effectiveness. Answer: D is incorrect. Metric thresholds are decision or action points that are enacted when a KPI or KRI reports a specific value or set of values.

QUESTION 301
What are the functions of the auditor while analyzing risk? Each correct answer represents a complete solution. Choose three.

A. Aids in determining audit objectives
B. Identify threats and vulnerabilities to the information system
C. Provide information for evaluation of controls in audit planning
D. Supporting decision based on risks

Correct Answer: ACD
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats. A risk from an organizational perspective consists of:
Threats to various processes of organization.
Threats to physical and information assets.
Likelihood and frequency of occurrence from threat.
Impact on assets from threat and vulnerability.
Risk analysis allows the auditor to do the following tasks :
Threats to various processes of organization.
Threats to physical and information assets.
Likelihood and frequency of occurrence from threat.
Impact on assets from threat and vulnerability.
Risk analysis allows the auditor to do the following tasks :
Identify threats and vulnerabilities to the enterprise and its information system. Provide information for evaluation of controls in audit planning.
Aids in determining audit objectives.
Supporting decision based on risks.
Answer: B is incorrect. Auditors identify threats and vulnerability not only in the IT but the whole enterprise as well.

QUESTION 302
Henry is the project manager of the QBG Project for his company. This project has a budget of $4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work. What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?

A. Cost change control system

B. Configuration management system

C. Scope change control system

D. Integrated change control

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The configuration management system ensures that proposed changes to the project's scope are reviewed and evaluated for their affect on the project's product. Configure management process is important in achieving business objectives. Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability minimizes production issues and resolves issues more quickly.
Answer: C is incorrect. The scope change control system focuses on reviewing the actual changes to the project scope. When a change to the project's scope is proposed, the configuration management system is also invoked.
Answer: A is incorrect. The cost change control system is responsible for reviewing and controlling changes to the project costs.
Answer: D is incorrect. Integrated change control examines the affect of a proposed change on the project as a whole.

QUESTION 303
What are the key control activities to be done to ensure business alignment? Each correct answer represents a part of the solution. Choose two.

A. Define the business requirements for the management of data by IT

B. Conduct IT continuity tests on a regular basis or when there are major changes in the IT infrastructure

C. Periodically identify critical data that affect business operations

D. Establish an independent test task force that keeps track of all events

Correct Answer: AC
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Business alignment require following control activities:
Defining the business requirements for the management of data by IT. Periodically identifying critical data that affect business operations, in alignment with the risk management model and IT service as well as the business continuity plan. Answer: B is incorrect. Conducting IT continuity tests on a regular basis or when there are major changes in the IT infrastructure is done for testing IT continuity plan. It does not ensure alignment with business.
Answer: D is incorrect. This is not valid answer.
TestsQuizNotesArticlesItemsReportsHelpBuy

QUESTION 304
Which of the following statements is true for risk analysis?

A. Risk analysis should assume an equal degree of protection for all assets.
B. Risk analysis should give more weight to the likelihood than the size of loss.
C. Risk analysis should limit the scope to a benchmark of similar companies
D. Risk analysis should address the potential size and likelihood of loss.

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
A risk analysis deals with the potential size and likelihood of loss. A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats. A risk from an organizational perspective consists of:
Threats to various processes of organization.
Threats to physical and information assets.
Likelihood and frequency of occurrence from threat.
Impact on assets from threat and vulnerability.
Risk analysis allows the auditor to do the following tasks :
Identify threats and vulnerabilities to the enterprise and its information system. Provide information for evaluation of controls in audit planning.
Aids in determining audit objectives.
Supporting decision based on risks.
Answer: B is incorrect. Since the likelihood determines the size of the loss, hence both elements must be considered in the calculation.
Answer: C is incorrect. A risk analysis would not normally consider the benchmark of similar companies as providing relevant information other than for comparison purposes. Answer: A is incorrect. Assuming equal degree of protection would only be rational in the rare event that all the assets are similar in sensitivity and criticality. Hence this is not practiced in risk analysis.

QUESTION 305
You are working in Bluewell Inc. which make advertisement Websites. Someone had made unauthorized changes to a your Website. Which of the following terms refers to this type of loss?

A. Loss of confidentiality
B. Loss of integrity
C. Loss of availability
D. Loss of revenue

Correct Answer: B

Section: Volume D
Explanation

Explanation/Reference:
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
Answer: A is incorrect. Someone sees a password or a company's secret formula, this is referred to as loss of confidentiality.
Answer: C is incorrect. An e-mail server is down and no one has e-mail access, or a file server is down so data files aren't available comes under loss of availability. Answer: D is incorrect. This refers to the events which would eventually cause loss of revenue.

QUESTION 306
Which of the following is NOT true for Key Risk Indicators?

A. They are selected as the prime monitoring indicators for the enterprise
B. They help avoid having to manage and report on an excessively large number of risk indicators
C. The complete set of KRIs should also balance indicators for risk, root causes and business impact.
D. They are monitored annually

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
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: A, B, and C 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 307
What are the responsibilities of the CRO?
Each correct answer represents a complete solution. Choose three.

A. Managing the supporting risk management function
B. Managing the risk assessment process

C. Advising Board of Directors

D. Implement corrective actions

Correct Answer: ABD
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Chief Risk Officer is the executive-level manager in an organization. They provide corporate, guidance, governance, and oversight over the enterprise's risk management activities. The main priority for the CRO is to ensure that the organization is in full compliance with applicable regulations. They may also deal with areas regarding insurance, internal auditing, corporate investigations, fraud, and information security.
CRO's responsibilities include:
Managing the risk assessment process
Implementation of corrective actions
Communicate risk management issues
Supporting the risk management functions

QUESTION 308
You are the project manager of the GHT project. You are accessing data for further analysis. You have chosen such a data extraction method in which management monitors its own controls. Which of the following data extraction methods you are using here?

A. Extracting data directly from the source systems after system owner approval

B. Extracting data from the system custodian (IT) after system owner approval

C. Extracting data from risk register

D. Extracting data from lesson learned register

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Direct extraction from the source system involves management monitoring its own controls, instead of auditors/third parties monitoring management's controls. It is preferable over extraction from the system custodian.
Answer: C and D are incorrect. These are not data extraction methods. Answer: B is incorrect. Extracting data from the system custodian (IT) after system owner approval, involves auditors or third parties monitoring management's controls. Here, in this management does not monitors its own control.

QUESTION 309
You are the project manager for your organization to install new workstations, servers, and cabling throughout a new building, where your company will be moving

into. The vendor for the project informs you that the cost of the cabling has increased due to the some reason. This new cost will cause the cost of your project to increase by nearly eight percent. What change control system should the costs be entered into for review?

A. Cost change control system
B. Contract change control system
C. Scope change control system
D. Only changes to the project scope should pass through a change control system.

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Because this change deals with the change of the deliverable, it should pass through the cost change control system. The cost change control system reviews the reason why the change has happened, what the cost affects, and how the project should respond. Answer: B is incorrect. This is not a contract change. According to the evidence that a contract exists or that the cost of the materials is outside of the terms of a contract if one existed. Considered a time and materials contract where a change of this nature could be acceptable according to the terms of the contract. If the vendor wanted to change the terms of the contract then it would be appropriate to enter the change into the contract change control system.
Answer: C is incorrect. The scope of the project will not change due to the cost of the materials.
Answer: D is incorrect. There are four change control systems that should always be entertained for change: schedule, cost, scope, and contract.

QUESTION 310
When a risk cannot be sufficiently mitigated through manual or automatic controls, which of the following options will BEST protect the enterprise from the potential financial impact of the risk?

A. Updating the IT risk registry
B. Insuring against the risk
C. Outsourcing the related business process to a third party
D. Improving staff-training in the risk area

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
An insurance policy can compensate the enterprise up to 100% by transferring the risk to another company. Hence in this stem risk is being transferred. Answer: A is incorrect. Updating the risk registry (with lower values for impact and probability) will not actually change the risk, only management's perception of it. Answer: D is incorrect. Staff capacity to detect or mitigate the risk may potentially reduce the financial impact, but insurance allows for the risk to be mitigated up to 100%.

Answer: C is incorrect. Outsourcing the process containing the risk does not necessarily remove or change the risk. While on other hand, insurance will completely remove the risk.

QUESTION 311
You are the risk official at Bluewell Inc. There are some risks that are posing threat on your enterprise. You are measuring exposure of those risk factors, which has the highest potential, by examining the extent to which the uncertainty of each element affects the object under consideration when all other uncertain elements are held at their baseline values. Which type of analysis you are performing?

A. Sensitivity analysis
B. Fault tree analysis
C. Cause-and-effect analysis
D. Scenario analysis

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Sensitivity analysis is the quantitative risk analysis technique that:
Assist in determination of risk factors that have the most potential impact Examines the extent to which the uncertainty of each element affects the object under consideration when all other uncertain elements are held at their baseline values Answer: B is incorrect. Fault tree analysis provides a systematic description of the combination of possible undesirable occurrences in a system. It does not measure the extent of uncertainty.
Answer: C is incorrect. Cause-and-effect 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, and not the extent of uncertainty. Answer: D is incorrect. Scenario analysis provides ability to see a range of values across several scenarios to identify risk in specific situation. It provides ability to identify those inputs which will provide the greatest level of uncertainty. But it plays no role in determining the extent of uncertainty.

QUESTION 312
Which of the following risk responses include feedback and guidance from well-qualified risk officials and those internal to the project?

A. Contingent response strategy
B. Risk Acceptance
C. Expert judgment
D. Risk transfer

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Expert judgment is utilized in developing risk responses, including feedback and guidance from risk management experts and those internal to the project qualified to provide assistance in this process. Expert judgment is a technique based on a set of criteria that has been acquired in a specific knowledge area or product area. It is obtained when the project manager or project team requires specialized knowledge that they do not possess. Expert judgment involves people most familiar with the work of creating estimates. Preferably, the project team member who will be doing the task should complete the estimates. Expert judgment is applied when performing administrative closure activities, and experts should ensure the project or phase closure is performed to the appropriate standards. Answer: B is incorrect. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs. If an enterprise adopts a risk acceptance, it should carefully consider who can accept the risk. Risk should be accepted only by senior management in relationship with senior management and the board. There are two alternatives to the acceptance strategy, passive and active.
Passive acceptance means that enterprise has made no plan to avoid or mitigate the risk but willing to accept the consequences of the risk.
Active acceptance is the second strategy and might include developing contingency plans and reserves to deal with risks.
Answer: D is incorrect. Risk transfer means that impact of risk is reduced by transferring or otherwise sharing a portion of the risk with an external organization or another internal entity. Transfer of risk can occur in many forms but is most effective when dealing with financial risks. Insurance is one form of risk transfer.
Answer: A is incorrect. Contingent response strategy, also known as contingency planning, involves adopting alternatives to deal with
the risks in case of their occurrence. Unlike the mitigation planning in which mitigation looks to reduce the probability of the risk and its impact, contingency planning doesn't necessarily attempt to reduce the probability of a risk event or its impacts. Contingency comes into action when the risk event actually occurs.

QUESTION 313
You are the risk professional of your enterprise. Your enterprise has introduced new systems in many departments. The business requirements that were to be addressed by the new system are still unfulfilled, and the process has been a waste of resources. Even if the system is implemented, it will most likely be underutilized and not maintained making it obsolete in a short period of time. What kind of risk is it?

A. Inherent risk
B. Business risk
C. Project risk
D. Residual risk

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Business risk relates to the likelihood that the new system may not meet the user business needs, requirements and expectations. Here in this stem it is said that the business requirements that were to be addressed by the new system are still unfulfilled, therefore it is a business risk.
Answer: A is incorrect. This is one of the components of risk. Inherent risk is the risk level or exposure without applying controls or other management actions into account. But here in this stem no description of control is given, hence it cannot be concluded whether it is a inherent risk or not.
Answer: C is incorrect. Project risk are related to the delay in project deliverables. The project activities to design and develop the system exceed the limits of the financial resources set aside for the project. As a result, the project completion will be delayed. They are not related to fulfillment of business requirements. Answer: D is incorrect. This is one of the components of risk. Residual risk is the risk that remains after applying controls.

But here in this stem no description of control is given, hence it cannot be concluded whether it is a residual risk or not.

QUESTION 314
Qualitative risk assessment uses which of the following terms for evaluating risk level? Each correct answer represents a part of the solution. Choose two.

A. Impact
B. Annual rate of occurrence
C. Probability
D. Single loss expectancy

Correct Answer: AC
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Unlike the quantitative risk assessment, qualitative risk assessment does not assign dollar values. Rather, it determines risk's level based on the probability and impact of a risk. These values are determined by gathering the opinions of experts. Probability- establishing the likelihood of occurrence and reoccurrence of specific risks, independently, and combined. The risk occurs when a threat exploits vulnerability. Scaling is done to define the probability that a risk will occur. The scale can be based on word values such as Low, Medium, or High. Percentage can also be assigned to these words, like 10% to low and 90% to high.
Impact- Impact is used to identify the magnitude of identified risks. The risk leads to some type of loss. However, instead of quantifying the loss as a dollar value, an impact assessment could use words such as Low, Medium, or High. Impact is expressed as a relative value. For example, low could be 10, medium could be 50, and high could be 100.
Risk level= Probability*Impact
Answer: D and B are incorrect. These are used for calculating Annual loss expectancy (ALE) in quantitative risk assessment. Formula is given as follows:
ALE= SLE*ARO

QUESTION 315
You are working in an enterprise. You enterprise is willing to accept a certain amount of risk.
What is this risk called?

A. Hedging
B. Aversion
C. Appetite
D. Tolerance

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Risk appetite considers the qualitative and quantitative aspects of accepting risks in an organization. The term refers to the type of risks the organization is willing to pursue, as well as amount of risk and the level of risk.
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. Answer: B and A are incorrect. Aversion and hedging are related to each other and represents the avoidance of risk within the organization.
Answer: D is incorrect. 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.

QUESTION 316
You are the project manager of the NNN Project. Stakeholders in the two-year project have requested to send status reports to them via. email every week. You have agreed and send reports every Thursday. After six months of the project, the stakeholders are pleased with the project progress and they would like you to reduce the status reports to every two weeks. What process will examine the change to this project process and implement it in the project?

A. Configuration management
B. Communications management
C. Perform integrated change control process
D. Project change control process

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Although this appears to be a simple change the project manager must still follow the rules of the project's change control system.
Integrated change control is a way to manage the changes incurred during a project. It is a method that manages reviewing the suggestions for changes and utilizing the tools and techniques to evaluate whether the change should be approved or rejected. Integrated change control is a primary component of the project's change control system that examines the affect of a proposed change on the entire project.
Answer: B is incorrect. Communications management is the execution of the communications management plan.
Answer: D is incorrect. The project change control process not valid as it's the parent of the integrated change control process, which is more accurate for this option A is incorrect. Configuration management is the documentation and control of the product's features and functions.

QUESTION 317
You are the project manager of your enterprise. You have identified several risks. Which of the following responses to risk is considered the MOST appropriate?

A. Any of the above

B. Insuring

C. Avoiding

D. Accepting

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The appropriate response to the risk is decided by the risk itself, the company's attitude and appetite of risk, and the threat and opportunity combination of the risk.
Answer: C, D, and B are incorrect. Depending upon the condition, that is, the risk itself, the company's attitude and appetite of risk, and the threat and opportunity combination of the risk, these response options can be chosen.

QUESTION 318
John is the project manager of the HGH Project for her company. He and his project team have agreed that if the vendor is late by more than ten days they will cancel the order and hire the NBG Company to fulfill the order. The NBG Company can guarantee orders within three days, but the costs of their products are significantly more expensive than the current vendor.
What type of response does John adopt here?

A. Contingent response strategy

B. Risk avoidance

C. Risk mitigation

D. Expert judgment

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
As in this case John and his team mates have pre-planned the alternative if the vendor would late in placing the order. Therefore, it is contingent response strategy.
Contingent response strategy, also known as contingency planning, involves adopting alternatives to deal with the risks in case of their occurrence. Unlike the mitigation planning in which mitigation looks to reduce the probability of the risk and its impact, contingency planning doesn't necessarily attempt to reduce the probability of a risk event or its impacts. Contingency comes into action when the risk event actually occurs. Answer: B is incorrect. Risk avoidance is the method which involves creating solutions that ensure a specific risk in not realized.
Answer: C is incorrect. Risk mitigation attempts to eliminate or significantly decrease the level of risk present. Here no alternatives are pre-planned. Answer: D is incorrect. Expert judgment is utilized in developing risk responses, including feedback and guidance from risk management experts and those internal to the project qualified to provide assistance in this process.

QUESTION 319
You work as a project manager for BlueWell Inc. You are preparing for the risk identification process. You will need to involve several of the project's key stakeholders to help you identify and communicate the identified risk events. You will also need several documents to help you and the stakeholders identify the risk events. Which one of the following is NOT a document that will help you identify and communicate risks within the project?

A. Stakeholder registers
B. Activity duration estimates
C. Activity cost estimates
D. Risk register

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Risk register is not an input to risk identification, but it is an output of risk identification. Answer: C, B, and A are incorrect. These are an input to risk identification. Identify Risks is the process of determining which risks may affect the project. It also documents risks' characteristics. The Identify Risks process is part of the Project Risk Management knowledge area. As new risks may evolve or become known as the project progresses through its life cycle, Identify Risks is an iterative process. The process should involve the project team so that they can develop and maintain a sense of ownership and responsibility for the risks and associated risk response actions. Risk Register is the only output of this process.

QUESTION 320
You work as a project manager for TechSoft Inc. You are working with the project stakeholders on the qualitative risk analysis process in youproject. You have used all the tools to the qualitative risk analysis process in your project. Which of the following techniques is NOT used asa tool in qualitative risk analysis process?

A. Risk Urgency Assessment
B. Risk Reassessment
C. Risk Data Quality Assessment
D. Risk Categorization

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
You will not need the Risk Reassessment technique to perform qualitative risk analysis. It is one of the techniques used to monitor and control risks.
Answer: D, A, and C are incorrect.
The tools and techniques for Qualitative Risk Analysis process are as follows :

Risk Probability and Impact Assessment: Risk probability assessment investigates the chances of a particular risk to occur.
Risk Impact Assessment investigates the possible effects on the project objectives such as cost, quality, schedule, or performance, including positive opportunities and negative threats. Probability and Impact Matrix: Estimation of risk's consequence and priority for awareness is conducted by using a look-up table or the probability and impact matrix. This matrix specifies the mixture of probability and impact that directs to rating the risks as low, moderate, or high priority.
Risk Data Quality Assessment: Investigation of quality of risk data is a technique to calculate the degree to which the data about risks are useful for risk management. Risk Categorization: Risks to the projects can be categorized by sources of risk, the area of project affected and other valuable types to decide the areas of the project most exposed to the effects of uncertainty.
Risk Urgency Assessment: Risks that requires near-term responses are considered more urgent to address.
Expert Judgment: It is required to categorize the probability and impact of each risk to determine its location in the matrix.

QUESTION 321
Which of the following is the greatest risk to reporting?

A. Integrity of data
B. Availability of data
C. Confidentiality of data
D. Reliability of data

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Reporting risks are caused due to wrong reporting which leads to bad decision. This bad decision due to wrong report hence causes a risk on the functionality of the organization. Therefore, the greatest risk to reporting is reliability of data. Reliability of data refers to the accuracy, robustness, and timing of the data.
Answer: A, B, and C are incorrect. Integrity, availability, and confidentiality of data are also important, but these three in combination comes under reliability itself.

QUESTION 322
Which negative risk response usually has a contractual agreement?

A. Sharing
B. Transference
C. Mitigation
D. Exploiting

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Transference is the risk response that transfers the risk to a third party, usually for a fee. Insurance and subcontracting of dangerous works are two common examples of transference with a contractual obligation.
Answer: C is incorrect. Mitigation is a negative risk response used to lower the probability and/or impact of a risk event.
Answer: A is incorrect. Sharing is a positive risk response. Note that sharing may also have contractual obligations, sometimes called teaming agreements.
Answer: D is incorrect. Exploiting is a positive risk response and not a negative response and doesn't have contractual obligations.

QUESTION 323
Which of the following is the MOST important aspect to ensure that an accurate risk register is maintained?

A. Publish the risk register in a knowledge management platform with workflow features that periodically contacts and polls risk assessors to ensure accuracy of content
B. Perform regular audits by audit personnel and maintain risk register
C. Submit the risk register to business process owners for review and updating
D. Monitor key risk indicators, and record the findings in the risk register

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
A knowledge management platform with workflow and polling feature will automate the process of maintaining the risk registers. Hence this ensures that an accurate and updated risk register is maintained.
Answer: C is incorrect. Business process owners typically cannot effectively identify risk to their business processes. They may not have the ability to be unbiased and may not have the appropriate skills or tools for evaluating risks.
Answer: B is incorrect. Audit personnel may not have the appropriate business knowledge in risk assessment, hence cannot properly identify risk. Regular audits may also cause hindrance to the business activities.
Answer: D is incorrect. Monitoring key risk indicators, and record the findings in the risk register will only provide insights to known and identified risk and will not account for obscure risk, i.e. , risk that has not been identified yet.

QUESTION 324
Which of the following test is BEST to map for confirming the effectiveness of the system access management process?

A. user accounts to human resources (HR) records.
B. user accounts to access requests.
C. the vendor database to user accounts.
D. access requests to user accounts.

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Tying user accounts to access requests confirms that all existing accounts have been approved. Hence, the effectiveness of the system access management process can be accounted.
Answer: D is incorrect. Tying access requests to user accounts confirms that all access requests have been processed; however, the test does not consider user accounts that have been established without the supporting access request. Answer: A is incorrect. Tying user accounts to human resources (HR) records confirms whether user accounts are uniquely tied to employees, not accounts for the effectiveness of the system access management process.
Answer: C is incorrect. Tying vendor records to user accounts may confirm valid accounts on an e-commerce application, but it does not consider user accounts that have been established without the supporting access request.

QUESTION 325
Which of the following is the way to verify control effectiveness?

A. The capability of providing notification of failure.
B. Whether it is preventive or detective.
C. Its reliability.
D. The test results of intended objectives.

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Control effectiveness requires a process to verify that the control process worked as intended and meets the intended control objectives.
Hence the test result of intended objective helps in verifying effectiveness of control. Answer: C is incorrect. Reliability is not an indication of control strength; weak controls can be highly reliable, even if they do not meet the control objective. Answer: B is incorrect. The type of control, like preventive or detective, does not help determine control effectiveness.
Answer: A is incorrect. Notification of failure does not determine control strength, hence this option is not correct.

QUESTION 326
What is the most important benefit of classifying information assets?

A. Linking security requirements to business objectives
B. Allotting risk ownership
C. Defining access rights

D. Identifying controls that should be applied

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
All of the options are directly or indirectly are the advantages of classifying information assets, but the most important benefit amongst them is that appropriate controls can be identified.
Answer: C, B, and A are incorrect. These all are less significant than identifying controls.

QUESTION 327
You are the project manager of GHT project. A risk event has occurred in your project and you have identified it. Which of the following tasks you would do in reaction to risk event occurrence? Each correct answer represents a part of the solution. Choose three.

A. Monitor risk
B. Maintain and initiate incident response plans
C. Update risk register
D. Communicate lessons learned from risk events

Correct Answer: ABD
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
When the risk events occur then following tasks have to done to react to it:
Maintain incident response plans
Monitor risk
Initiate incident response
Communicate lessons learned from risk events
Answer: C is incorrect. Risk register is updated after applying appropriate risk response and at the time of risk event occurrence.

QUESTION 328
Which of the following parameters would affect the prioritization of the risk responses and development of the risk response plan? Each correct answer represents a complete solution.
Choose three.

A. Importance of the risk

B. Time required to mitigate risk.

C. Effectiveness of the response

D. Cost of the response to reduce risk within tolerance levels

Correct Answer: ACD
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The prioritization of the risk responses and development of the risk response plan is influenced by several parameters:
Cost of the response to reduce risk within tolerance levels Importance of the risk
Capability to implement the response
Effectiveness of the response
Efficiency of the response
Answer: B is incorrect. Time required to mitigate risk does not influence the prioritization of the risk and development of the risk response plan. It affects the scheduled time of the project.

QUESTION 329
Which of the following come under the management class of controls? Each correct answer represents a complete solution. Choose all that apply.

A. Risk assessment control

B. Audit and accountability control

C. Program management control

D. Identification and authentication control

Correct Answer: AC
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The Management class of controls includes five families. These families include over 40 individual controls. Following is a list of each of the families in the Management class:
Certification, Accreditation, and Security Assessment (CA): This family of controls addresses steps to implement a security and assessment program. It includes controls to ensure only authorized systems are allowed on a network. It includes details on important security concepts, such as continuous monitoring and a plan of action and milestones. Planning (PL): The PL family focuses on security plans for systems. It also covers Rules of Behaviour for users. Rules of Behaviour are also called an acceptable use policy. Risk Assessment (RA): This family of controls provides details on risk assessments and vulnerability scanning.
System and Services Acquisition (SA): The SA family includes any controls related to the purchase of products and services. It also includes controls related to software usage and user installed software.

Program Management (PM): This family is driven by the Federal Information Security Management Act (FISMA). It provides controls to ensure compliance with FISMA. These controls complement other controls. They don't replace them. Answer: D and B are incorrect. Identification and authentication, and audit and accountability control are technical class of controls.

QUESTION 330
Which of the following parameters are considered for the selection of risk indicators? Each correct answer represents a part of the solution. Choose three.

A. Size and complexity of the enterprise
B. Type of market in which the enterprise operates
C. Risk appetite and risk tolerance
D. Strategy focus of the enterprise

Correct Answer: ABD
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Risk indicators are placed at control points within the enterprise and are used to collect data. These collected data are used to measure the risk levels at that point. They also track events or incidents that may indicate a potentially harmful situation. Risk indicators can be in form of logs, alarms and reports. Risk indicators are selected depending on a number of parameters in the internal and external environment, such as:
Size and complexity of the enterprise
Type of market in which the enterprise operates
Strategy focus of the enterprise
Answer: C is incorrect. Risk appetite and risk tolerance are considered when applying various risk responses.

QUESTION 331
David is the project manager of HRC project. He concluded while HRC project is in process that if he adopts e-commerce, his project can be more fruitful. But he did not engaged in electronic commerce (e-commerce) so that he would escape from risk associated with that line of business. What type of risk response had he adopted?

A. Acceptance
B. Avoidance
C. Exploit
D. Enhance

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
As David did not engaged in e-commerce in order to avoid risk, hence he is following risk avoidance strategy.

QUESTION 332
Which of the following is the final step in the policy development process?

A. Management approval
B. Continued awareness activities
C. Communication to employees
D. Maintenance and review

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Organizations should create a structured ISG document development process. A formal process gives many areas the opportunity to comment on a policy. This is very important for high-level policies that apply to the whole organization. A formal process also makes sure that final policies are communicated to employees. It also provides organizations with a way to make sure that policies are reviewed regularly.
In general, a policy development process should include the following steps:
In general, a policy development process should include the following steps:
1.Development
2.Stakeholder review
3.Management approval
4.Communication to employees
5.Documentation of compliance or exceptions
6.Continued awareness activities
7.Maintenance and review
Answer: A, B, and C are incorrect. These are the earlier phases in policy development process.

QUESTION 333
You are the project manager of GHT project. Your project utilizes a machine for production of goods. This machine has the specification that if its temperature would rise above 450 degree Fahrenheit then it may result in burning of windings. So, there is an alarm which blows when machine's temperature reaches 430 degree Fahrenheit and the machine is shut off for 1 hour. What role does alarm contribute here?

A. Of risk indicator
B. Of risk identification
C. Of risk trigger

D. Of risk response

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Here in this scenario alarm indicates the potential risk that the rising temperature of machine can cause, hence it is enacting as a risk indicator. Risk indicators are metrics used to indicate risk thresholds, i.e., it gives indication when a risk level is approaching a high or unacceptable level of risk. The main objective of a risk indicator is to ensure tracking and reporting mechanisms that alert staff about the potential risks.
Answer: C is incorrect. The temperature 430 degree in scenario is the risk trigger. A risk trigger is a warning sign or condition that a risk event is about to happen. As in this scenario the 430 degree temperature is the indication of upcoming risks, hence 430 degree temperature is a risk trigger.
Answer: D is incorrect. Risk response is the action taken to reduce the risk event occurrence. Hence here risk response is shutting off of machine. Answer: B is incorrect. The first thing we must do in risk management is to identify the areas of the project where the risks can occur. This is termed as risk identification. Listing all the possible risks is proved to be very productive for the enterprise as we can cure them before it can occur. In risk identification both threats and opportunities are considered, as both carry some level of risk with them.

QUESTION 334
When does the Identify Risks process take place in a project?

A. At the Planning stage.
B. At the Executing stage.
C. At the Initiating stage.
D. Throughout the project life-cycle.

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Identify Risks is the process of determining which risks may affect the project. It also documents risks' characteristics. The Identify Risks process is part of the Project Risk Management knowledge area. As new risks may evolve or become known as the project progresses through its life cycle, Identify Risks is an iterative process. The process should involve the project team so that they can develop and maintain a sense of ownership and responsibility for the risks and associated risk response actions. Risk Register is the only output of this process.
Answer: C, A, and B are incorrect. Identify Risks process takes place at all the stages of a project, because risk changes over time.

QUESTION 335
In the project initiation phase of System Development Life Cycle, there is information on project initiated by which of the following role carriers?

A. CRO
B. Sponsor
C. Business management
D. CIO

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Project initiation section of SDLC contains information on projects initiated by sponsors who gather the information required to gain approval for the project to be created.

QUESTION 336
Which of the following are the responsibilities of Enterprise risk committee? Each correct answer represents a complete solution. Choose three.

A. React to risk events
B. Analyze risk
C. Risk aware decision
D. Articulate risk

Correct Answer: BCD
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Risk aware decision, analyzing risk, and articulating risk are the responsibilities of Enterprise risk committee. They are the executives who are accountable for the enterprise level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions. An IT risk council may be established to consider IT risk in more detail and advise the enterprise risk committee. ERC ensure that these activities are completed successfully.
Answer: A is incorrect. ERM is not responsible for reaction over risk events. Business process owners are accounted for this task.

QUESTION 337
Malicious code protection is which type control?

A. Configuration management control
B. System and information integrity control
C. Media protection control

D. Personal security control

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Malware, short for malicious software, is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems. As malicious code protection lists steps to protect against malware, it preserves the information integrity of the enterprise.
Hence Malicious code protection is System and information integrity control. This family of controls provides information to maintain the integrity of systems and data. Answer: D is incorrect. Malicious code protection is not a Personal security control. The Personal security control is a family of controls including aspects of personnel security. It includes personnel screening, termination, and transfer. Answer: A is incorrect. Malicious code protection is not a Configuration management control.
Configuration management control is the family of controls that addresses both configuration management and change management. Change control practices prevent unauthorized changes.
Answer: C is incorrect. Malicious code protection is not a Media protection control. Media Protection includes removable digital media such as tapes, external hard drives, and USB flash drives. It also includes non-digital media such as paper and film. This family of controls covers the access, marking, storage, transport, and sanitization of media.

QUESTION 338
If one says that the particular control or monitoring tool is sustainable, then it refers to what ability?

A. The ability to adapt as new elements are added to the environment
B. The ability to ensure the control remains in place when it fails
C. The ability to protect itself from exploitation or attack
D. The ability to be applied in same manner throughout the organization

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Sustainability of the controls or monitoring tools refers to its ability to function as expected over time or when changes are made to the environment. Answer: D is incorrect. This is not valid definition for defining sustainability of al tool. Answer: B is incorrect. Sustainability ensures that controls changes with the conditions, so as not to fail in any circumstances. Hence this in not valid answer.
Answer: C is incorrect. This in not valid answer.

QUESTION 339
You work as a Project Manager for Company Inc. You are incorporating a risk response owner to take the job for each agreed-to and funded risk response. On

which of the following processes are you working?

A. Quantitative Risk Analysis
B. Identify Risks
C. Plan risk response
D. Qualitative Risk Analysis

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
The plan risk response project management process aims to reduce the threats to the project objectives and to increase opportunities. It follows the perform qualitative risk analysis process and perform quantitative risk analysis process. Plan risk response process includes the risk response owner to take the job for each agreed-to and funded risk response. This process addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget. The inputs to the plan risk response process are as follows:
Risk register
Risk management plan
Answer: B is incorrect. Identify Risks is the process of determining which risks may affect the project. It also documents risks' characteristics. The Identify Risks process is part of the Project Risk Management knowledge area. As new risks may evolve or become known as the project progresses through its life cycle, Identify Risks is an iterative process. The process should involve the project team so that they can develop and maintain a sense of ownership and responsibility for the risks and associated risk response actions. Risk Register is the only output of this process.
Answer: A is incorrect. 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: D is incorrect. Qualitative analysis is the definition of risk factors in terms of high/medium/low or a numeric scale (1 to 10).
Hence it determines the nature of risk on a relative scale. Some of the qualitative methods of risk analysis are:
Scenario analysis- This is a forward-looking process that can reflect risk for a given point in time.
Risk Control Self -assessment (RCSA) - RCSA is used by enterprises (like banks) for the identification and evaluation of operational risk exposure. It is a logical first step and assumes that business owners and managers are closest to the issues and have the most expertise as to the source of the risk. RCSA is a constructive process in compelling business owners to contemplate, and then explain, the issues at hand with the added benefit of increasing their accountability.

QUESTION 340
Which of the following is NOT the method of Qualitative risk analysis?

A. Scorecards
B. Attribute analysis

C. Likelihood-impact matrix

D. Business process modeling (BPM) and simulation

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Business process modeling (BPM) and simulation is a method of Quantitative risk analysis and not Qualitative risk analysis.
The BPM and simulation discipline is an effective method of identifying and quantifying the operational risk in enterprise business processes.
It improves business process efficiency and effectiveness. Answer: A, C, and B are incorrect. These three are the methods of Qualitative risk analysis.

QUESTION 341
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. $ 108,000

D. $ 90,000

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
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 342
Which of the following is a performance measure that is used to evaluate the efficiency of an investment or to compare the efficiency of a number of different investments?

A. Return On Security Investment
B. Total Cost of Ownership
C. Return On Investment
D. Redundant Array of Inexpensive Disks

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Return On Investment (ROI) is a performance measure used to evaluate the efficiency of an investment or to compare the efficiency of a number of different investments. To calculate ROI, the benefit (return) of an investment is divided by the cost of the investment; the result is expressed as a percentage or a ratio.
The return on investment formula:
ROI= (Gain from investment - Cost of investment) / Cost of investment In the above formula "gains from investment", refers to the proceeds obtained from selling the investment of interest.
Answer: D is incorrect. RAID is described as a redundant array of inexpensive disks. It is a technology that allows computer users to achieve high levels of storage reliability from low- cost and less reliable PC-class disk-drive components, via the technique of arranging the devices into arrays for redundancy.
Answer: A and B are incorrect. These options are not related to the measurement of efficiency of an investment.

QUESTION 343
You are the program manager for your organization and you are working with Alice, a project manager in her program. Alice calls you and insists you to add a change to program scope. You agree for that the change. What must Alice do to move forward with her change request?

A. Add the change to the program scope herself, as she is a project manager
B. Create a change request charter justifying the change request
C. Document the change request in a change request form.
D. Add the change request to the scope and complete integrated change control

Correct Answer: C
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Change requests must be documented to be considered. Alice should create a change request form and follow the procedures of the change control system.

QUESTION 344
Which of the following business requirements MOST relates to the need for resilient business and information systems processes?

A. Confidentiality
B. Effectiveness
C. Integrity
D. Availability

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Availability relates to information being available when required by the business process in present as well as in future. Resilience is the ability to provide and maintain an acceptable level of service during disasters or when facing operational challenges. Hence they are most closely related.
Answer: B is incorrect. Confidentiality deals with the protection of sensitive information from unauthorized disclosure. While the lack of system resilience can in some cases affect data confidentiality, resilience is more closely linked to the business information requirement of availability.
Answer: A is incorrect. Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations. While the lack of system resilience can in some cases affect data integrity, resilience is more closely linked to the business information requirement of availability. Answer: C is incorrect. Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner. While the lack of system resilience can in some cases affect effectiveness, resilience is more closely linked to the business information requirement of availability.

QUESTION 345
Which of the following serve as the authorization for a project to begin?

A. Approval of project management plan
B. Approval of a risk response document
C. Approval of risk management document
D. Approval of a project request document

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Approval of a project initiation document (PID) or a project request document (PRD) is the authorization for a project to begin.

Answer: C is incorrect. Risk management document is being prepared later after the project initiation, during the risk management plan. It has no scope during project initialization. Answer: B is incorrect. Risk response document comes under risk management process, hence the latter phase in project development process. Answer: A is incorrect. Project management plan is being made after the project is being authorized.

QUESTION 346
In which of the following conditions business units tend to point the finger at IT when projects are not delivered on time?

A. Threat identification in project
B. System failure
C. Misalignment between real risk appetite and translation into policies
D. Existence of a blame culture

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
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.
Answer: B, C, and A are incorrect. These are not relevant to the pointing of finger at IT when projects are not delivered on time.

QUESTION 347
Which of the following methods involves the use of predictive or diagnostic analytical tool for exposing risk factors?

A. Scenario analysis
B. Sensitivity analysis
C. Fault tree analysis
D. Cause and effect analysis

Correct Answer: D
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Cause-and-effect 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. These tools also help in identifying potential risk. Answer: B is incorrect. Sensitivity analysis is the quantitative risk analysis technique that: Assist in determination of risk factors that have the most potential impact Examines the extent to which the uncertainty of each element affects the object under

consideration when all other uncertain elements are held at their baseline values Answer: C is incorrect. Fault tree analysis (FIA) is a technique that provides a systematic description of the combination of possible occurrences in a system, which can result in an undesirable outcome. It combines hardware failures and human failures. Answer: A is incorrect. This analysis is not a method for exposing risk factors. It is used for analyzing scenarios.

QUESTION 348
Sammy is the project manager for her organization. She would like to rate each risk based on its probability and affect on time, cost, and scope. Harry, a project team member, has never done this before and thinks Sammy is wrong to attempt this approach. Harry says that an accumulative risk score should be created, not three separate risk scores. Who is correct in this scenario?

A. Sammy is correct, because she is the project manager.
B. Sammy is correct, because organizations can create risk scores for each objective of the project.
C. Harry is correct, the risk probability and impact matrix is the only approach to risk assessment.
D. Harry is correct, because the risk probability and impact considers all objectives of the project.

Correct Answer: B
Section: Volume D
Explanation

Explanation/Reference:
Explanation:
Sammy She certainly can create an assessment for a risk event for time cost, and scope. It is probable that a risk event may have an effect on just one or more objectives so an assessment of the objective is acceptable.
Answer: A is incorrect. Just because Sammy is the project manager, it is not necessary that she is right.
Answer: D is incorrect. Harry's reasoning is flawed as each objective can be reviewed for the risk's impact rather than the total project.
Answer: C is incorrect. Harry is incorrect as there are multiple approaches to risk assessment for a project

QUESTION 349
Which of the following terms is described in the statement below? "They are the prime monitoring indicators of the enterprise, and are highly relevant and possess a high probability of predicting or indicating important risk. "

A. Key risk indicators
B. Lag indicators
C. Lead indicators
D. Risk indicators

Correct Answer: A
Section: Volume D
Explanation

Explanation/Reference:

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.
Answer: D is incorrect. Risk indicators are metrics used to indicate risk thresholds, i.e., it gives indication when a risk level is approaching a high or unacceptable level of risk. The main objective of a risk indicator is to ensure tracking and reporting mechanisms that alert staff about the potential risks.
Answer: C is incorrect. Lead indicators are the risk indicators that is used to indicate which capabilities are in place to prevent events from occurring. Answer: B is incorrect. Lag indicators are the risk indicators that is used to indicate risk after events have occurred.

QUESTION 350
Which of the following are true for quantitative analysis? Each correct answer represents a complete solution. Choose three.

A. Determines risk factors in terms of high/medium/low.
B. Produces statistically reliable results
C. Allows discovery of which phenomena are likely to be genuine and which are merely chance occurrences
D. Allows data to be classified and counted

Correct Answer: BCD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
As quantitative analysis is data driven, it:
Allows data classification and counting.
Allows statistical models to be constructed, which help in explaining what is being observed. Generalizes findings for a larger population and direct comparisons between two different sets of data or observations.
Produces statistically reliable results.
Allows discovery of phenomena which are likely to be genuine and merely occurs by chance. Answer: is incorrect. Risk factors are expressed in terms of high/ medium/low in qualitative analysis, and not in quantitative analysis.

QUESTION 351
Ned is the project manager of the HNN project for your company. Ned has asked you to help him complete some probability distributions for his project. What portion of the project will you most likely use for probability distributions?

A. Bias towards risk in new resources
B. Risk probability and impact matrixes
C. Uncertainty in values such as duration of schedule activities
D. Risk identification

Correct Answer: C

Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Risk probability distributions are likely to be utilized in uncertain values, such as time and cost estimates for a project.
Answer: D is incorrect. Risk probability distributions are not likely the risk identification. Answer: B is incorrect. Risk probability distributions are not likely to be used with risk probability and impact matrices.
Answer: A is incorrect. Risk probability distributions do not typically interact with the bias towards risks in new resources.

QUESTION 352
To which level the risk should be reduced to accomplish the objective of risk management?

A. To a level where ALE is lower than SLE
B. To a level where ARO equals SLE
C. To a level that an organization can accept
D. To a level that an organization can mitigate

Correct Answer: C
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The main objective of risk management is to reduce risk to a level that the organization or company will accept, as the risk can never be completely eliminated.
Answer: D is incorrect. Risk mitigation involves identification, planning, and conduct of actions for reducing risk. Because the elimination of all risk is usually impractical or close to impossible, it is aimed at reducing risk to an acceptable level with minimal adverse impact on the organization's resources and mission.
Answer: B and A are incorrect. There are no such concepts existing in manipulating risk level.

QUESTION 353
You are the project manager of GHT project. Your hardware vendor left you a voicemail saying that the delivery of the equipment you have ordered would not arrive on time. You identified a risk response strategy for this risk and have arranged for a local company to lease you the needed equipment until yours arrives. This is an example of which risk response strategy?

A. Avoid
B. Transfer
C. Acceptance
D. Mitigate

Correct Answer: D

Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Mitigation attempts to reduce the impact of a risk event in case it occurs. Making plans to arrange for the leased equipment reduces the consequences of the risk and hence this response in mitigation.
Answer: B is incorrect. Risk transfer means that impact of risk is reduced by transferring or otherwise sharing a portion of the risk with an external organization or another internal entity. Transfer of risk can occur in many forms but is most effective when dealing with financial risks. Insurance is one form of risk transfer.
Here there no such action is taken, hence it is not a risk transfer. Answer: C is incorrect. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs. If an enterprise adopts a risk acceptance, it should carefully consider who can accept the risk. Risk should be accepted only by senior management in relationship with senior management and the board. There are two alternatives to the acceptance strategy, passive and active.
Passive acceptance means that enterprise has made no plan to avoid or mitigate the risk but willing to accept the consequences of the risk.
Active acceptance is the second strategy and might include developing contingency plans and reserves to deal with risks.
Answer: A is incorrect. Risk avoidance means to evade risk altogether, eliminate the cause of the risk event, or change the project plan to protect the project objectives from the risk event. Risk avoidance is applied when the level of risk, even after the applying controls, would be greater than the risk tolerance level of the enterprise. Hence this risk response is adopted when:
There is no other cost-effective response that can successfully reduce the likelihood and magnitude below the defined thresholds for risk appetite.
The risk cannot be shared or transferred.
The risk is deemed unacceptable by management.

QUESTION 354
What should be considered while developing obscure risk scenarios? Each correct answer represents a part of the solution. Choose two.

A. Visibility
B. Controls
C. Assessment methods
D. Recognition

Correct Answer: AD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
The enterprise must consider risk that has not yet occurred and should develop scenarios around unlikely, obscure or non-historical events.
Such scenarios can be developed by considering two things:
Visibility
Recognition
For the fulfillment of this task enterprise must:
Be in a position that it can observe anything going wrong Have the capability to recognize an observed event as something wrong

QUESTION 355
Which of the following is true for risk management frameworks, standards and practices? Each correct answer represents a part of the solution. Choose three.

A. They act as a guide to focus efforts of variant teams.
B. They result in increase in cost of training, operation and performance improvement.
C. They provide a systematic view of "things to be considered" that could harm clients or an enterprise.
D. They assist in achieving business objectives quickly and easily.

Correct Answer: AD
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Frameworks, standards and practices are necessary as:
They provide a systematic view of "things to be considered" that could harm clients or an enterprise.
They act as a guide to focus efforts of variant teams. They save time and revenue, such as training costs, operational costs and performance improvement costs.
They assist in achieving business objectives quickly and easily.

QUESTION 356
An interruption in business productivity is considered as which of the following risks?

A. Reporting risk
B. Operational risk
C. Legal risk
D. Strategic risk

Correct Answer: B
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
Operation risks encompass any potential interruption in business. Operational risks are those risk that are associated with the day-to-day operations of the enterprise. They are generally more detailed as compared to strategic risks. It is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Some sub-categories of operational risks include:
Organizational or management related risks
Information security risks
Production, process, and productivity risks

Profitability operational risks
Business interruption risks
Project activity risks
Contract and product liability riss
Incidents and crisis
Illegal or malicious acts
Answer: D is incorrect. Strategic risks have potential which breaks in obtaining strategic objectives. Since the strategic objective will shape and impact the entire organization, the risk of not meeting that objective can impose a great threat on the organization. Answer: A is incorrect. Reporting risks are those occurrences which prevent accurate and timely reporting.
Answer: C is incorrect. Legal risks are dealing with those events which can deteriorate the company's legal status. Legal compliance is the process or procedure to ensure that an organization follows relevant laws, regulations and business rules. The definition of legal compliance, especially in the context of corporate legal departments, has recently been expanded to include understanding and adhering to ethical codes within entire professions, as well.
Hence legal and compliance risk has the potential to deteriorate company's legal or regulatory status.

QUESTION 357
You are the project manager of the QPS project. You and your project team have identified a pure risk. You along with the key stakeholders, decided to remove the pure risk from the project by changing the project plan altogether. What is a pure risk?

A. It is a risk event that only has a negative side and not any positive result.
B. It is a risk event that is created by the application of risk response.
C. It is a risk event that is generated due to errors or omission in the project work.
D. It is a risk event that cannot be avoided because of the order of the work.

Correct Answer: A
Section: Volume C
Explanation

Explanation/Reference:
Explanation:
A pure risk has only a negative effect on the project. Pure risks are activities that are dangerous to complete and manage such as construction, electrical work, or manufacturing. It is a class of risk in which loss is the only probable result and there is no positive result. Pure risk is associated to the events that are outside the risk-taker's control. Answer: D is incorrect. This in not valid definition of pure risk. Answer: B is incorrect. The risk event created by the application of risk response is called secondary risk.
Answer: C is incorrect. A risk event that is generated due to errors or omission in the project work is not necessarily pure risk.

QUESTION 358
Which of the following are the principles of access controls? Each correct answer represents a complete solution. Choose three.

A. Confidentiality
B. Availability

C. Reliability
D. Integrity

Correct Answer: ABD
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The principles of access controls focus on availability, integrity, and confidentiality, as loss or danger is directly related to these three:
Loss of confidentiality- Someone sees a password or a company's secret formula, this is referred to as loss of confidentiality.
Loss of integrity- An e-mail message is modified in transit, a virus infects a file, or someone makes unauthorized changes to a Web site is referred to as loss of integrity. Loss of availability- An e-mail server is down and no one has e-mail access, or a file server is down so data files aren't available comes under loss of availability.

QUESTION 359
You are the project manager of GHT project. You have selected appropriate Key Risk Indicators for your project. Now, you need to maintain those Key Risk Indicators. What is the MOST important reason to maintain Key Risk Indicators?

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

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Since the enterprise's internal and external environments are constantly changing, the risk environment is also highly dynamic, i.e., threats and vulnerabilities change over time. Hence KRIs need to be maintained to ensure that KRIs continue to effectively capture these changes.
Answer: A is incorrect. Timely risk reporting is one of the business requirements, but is not the reason behind KRI maintenance.
Answer: B is incorrect. While most key risk indicator 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. Answer: D is incorrect. Avoiding risk is a type of risk response. Risk responses are based on KRI reporting.

QUESTION 360
Which of the following controls do NOT come under technical class of control?

A. Program management control
B. System and Communications Protection control
C. Identification and Authentication control
D. Access Control

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Program Management control comes under management class of controls, not technical. Program Management control is driven by the Federal Information Security Management Act (FISMA). It provides controls to ensure compliance with FISMA. These controls complement other controls. They don't replace them.
Answer: D, C, and B are incorrect. These controls comes under technical class of control. The Technical class of controls includes four families. These families include over 75 individual controls. Following is a list of each of the families in the Technical class:
Access Control (AC): This family of controls 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 (AU): This 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.
Identification and Authentication (IA): These controls cover different practices to identify and authenticate users. Each user should be uniquely identified. In other words, each user has one account. This account is only used by one user. Similarly, device identifiers uniquely identify devices on the network.
System and Communications Protection (SC): The SC family is a large group of controls that cover many aspects of protecting systems and communication channels. Denial of service protection and boundary protection controls are included. Transmission integrity and confidentiality controls are also included.

QUESTION 361
Mary is a project manager in her organization. On her current project she is working with her project team and other key stakeholders to identify the risks within the project. She is currently aiming to create a comprehensive list of project risks so she is using a facilitator to help generate ideas about project risks. What risk identification method is Mary likely using?

A. Delphi Techniques
B. Expert judgment
C. Brainstorming
D. Checklist analysis

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:

Mary is using brainstorming in this example. Brainstorming attempts to create a comprehensive list of risks and often is led by a moderator or facilitator to move the process along.
Brainstorming is a technique to gather general data. It can be used to identify risks, ideas, or solutions to issues by using a group of team members or subject-matter expert. Brainstorming is a group creativity technique that also provides other benefits, such as boosting morale, enhancing work enjoyment, and improving team work.
Answer: D is incorrect. Checklist analysis uses historical information and information from similar projects within the organization's experience. Answer: A is incorrect. The Delphi technique uses rounds of anonymous surveys to generate a consensus on the identified risks.
Answer: B is incorrect. Expert judgment is not the best answer for this; projects experts generally do the risk identification, in addition to the project team.

QUESTION 362
Which of the following is an administrative control?

A. Water detection
B. Reasonableness check
C. Data loss prevention program
D. Session timeout

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:

QUESTION 363
You are the project manager of the NHH Project. You are working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document do you and your team is creating in this scenario?

A. Project plan
B. Resource management plan
C. Project management plan
D. Risk management plan

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:

The risk management plan, part of the comprehensive management plan, defines how risks will be identified, analyzed, monitored and controlled, and even responded to. A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix.
Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for project execution.
Answer: C is incorrect. The project management plan is a comprehensive plan that communicates the intent of the project for all project management knowledge areas. Answer: A is incorrect. The project plan is not an official PMBOK project management plan. Answer: B is incorrect. The resource management plan defines the management of project resources, such as project team members, facilities, equipment, and contractors.

QUESTION 364
An enterprise has identified risk events in a project. While responding to these identified risk events, which among the following stakeholders is MOST important for reviewing risk response options to an IT risk.

A. Information security managers
B. Internal auditors
C. Incident response team members
D. Business managers

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Business managers are accountable for managing the associated risk and will determine what actions to take based on the information provided by others.
Answer: A is incorrect. Information security managers may best understand the technical tactical situation, but business managers are accountable for managing the associated risk and will determine what actions to take based on the information provided by others, which includes collaboration with, and support from, IT security managers. Answer: C is incorrect. The incident response team must ensure open communication to management and stakeholders to ensure that business managers understand the associated risk and are provided enough information to make informed risk-based decisions. They are not responsible for reviewing risk response options.

QUESTION 365
Which of the following is a technique that provides a systematic description of the combination of unwanted occurrences in a system?

A. Sensitivity analysis
B. Scenario analysis
C. Fault tree analysis
D. Cause and effect analysis

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Fault tree analysis (FIA) is a technique that provides a systematic description of the combination of possible occurrences in a system, which can result in an undesirable outcome.
It combines hardware failures and human failures.
Answer: B is incorrect. This analysis provides ability to see a range of values across several scenarios to identify risk in specific situation. It provides ability to identify those inputs which will provide the greatest level of uncertainty. Answer: D is incorrect. Cause-and-effect 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. These tools also help in identifying potential risk. Answer: A is incorrect. Sensitivity analysis is the quantitative risk analysis technique that:
Assist in determination of risk factors that have the most potential impact Examines the extent to which the uncertainty of each element affects the object under consideration when all other uncertain elements are held at their baseline values

QUESTION 366
What is the process for selecting and implementing measures to impact risk called?

A. Risk Treatment
B. Control
C. Risk Assessment
D. Risk Management

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The process for selecting and implementing measures for impacting risk in the environment is called risk treatment.
Answer: A is incorrect. Risk management is the coordinated activities for directing and controlling the treatment of risk in the organization. Answer: C is incorrect. The process of analyzing and evaluating risk is called risk assessment.

QUESTION 367
Which section of the Sarbanes-Oxley Act specifies "Periodic financial reports must be certified by CEO and CFO"?

A. Section 302
B. Section 404

C. Section 203
D. Section 409

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Section 302 of the Sarbanes-Oxley Act requires corporate responsibility for financial reports to be certified by CEO, CFO, or designated representative. Answer: C is incorrect. Section 203 of the Sarbanes-Oxley Act requires audit partners and review partners to rotate off an assignment every five years. Answer: D is incorrect. Section 409 of the Sarbanes-Oxley Act states that the financial reports must be distributed quickly and currently.
Answer: B is incorrect. Section 404 of the Sarbanes-Oxley Act states that annual assessments of internal controls are the responsibility of management.

QUESTION 368
What is the PRIMARY need for effectively assessing controls?

A. Control's alignment with operating environment
B. Control's design effectiveness
C. Control's objective achievement
D. Control's operating effectiveness

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Controls can be effectively assessed only by determining how accurately the control objective is achieved within the environment in which they are operating. No conclusion can be reached as to the strength of the control until the control has been adequately tested. Answer: B is incorrect. Control's design effectiveness is also considered but is latter considered after achieving objectives.
Answer: D is incorrect. Control's operating effectiveness is considered but after its accuracy in objective achievement.
Answer: A is incorrect. Alignment of control with the operating environment is essential but after the control's accuracy in achieving objective. In other words, achieving objective is the top most priority in assessing controls.

QUESTION 369
You work as the project manager for Bluewell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decide, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project, what is likely to increase?

A. Human resource needs

B. Quality control concerns

C. Costs

D. Risks

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
Fast tracking allows entire phases of the project to overlap and generally increases risks within the project.
Fast tracking is a technique for compressing project schedule. In fast tracking, phases are overlapped that would normally be done in sequence. It is shortening the project schedule without reducing the project scope.
Answer: B is incorrect. Quality control concerns usually are not affected by fast tracking decisions.
Answer: C is incorrect. Costs do not generally increase based on fast tracking decisions. Answer: A is incorrect. Human resources are not affected by fast tracking in most scenarios.

QUESTION 370
David is the project manager of the HRC Project. He has identified a risk in the project, which could cause the delay in the project. David does not want this risk event to happen so he takes few actions to ensure that the risk event will not happen. These extra steps, however, cost the project an additional $10,000. What type of risk response has David adopted?

A. Avoidance

B. Mitigation

C. Acceptance

D. Transfer

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
As David is taking some operational controls to reduce the likelihood and impact of the risk, hence he is adopting risk mitigation. Risk mitigation means that actions are taken to reduce the likelihood and/or impact of risk.
Answer: C is incorrect. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted in case it occurs. As David has taken some actions in case to defend, therefore he is not accepting risk.
Answer: A is incorrect. Risk avoidance means that activities or conditions that give rise to risk are discontinued. But here, no such actions are taken, therefore risk in not avoided. Answer: D is incorrect. David has not hired a vendor to manage the risk for his project; therefore he is not transferring the risk.

QUESTION 371
Which of the following is the MOST important objective of the information system control?

A. Business objectives are achieved and undesired risk events are detected and corrected
B. Ensuring effective and efficient operations
C. Developing business continuity and disaster recovery plans
D. Safeguarding assets

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The basic purpose of Information System control in an organization is to ensure that the business objectives are achieved and undesired risk events are detected and corrected. Some of the IS control objectives are given below :
Safeguarding assets
Assuring integrity of sensitive and critical application system environments Assuring integrity of general operating system
Ensuring effective and efficient operations
Fulfilling user requirements, organizational policies and procedures, and applicable laws and regulations
Changing management
Developing business continuity and disaster recovery plans Developing incident response and handling plans
Hence the most important objective is to ensure that business objectives are achieved and undesired risk events are detected and corrected.
Answer: B, D, and C are incorrect. These are also the objectives of the information system control but are not the best answer.

QUESTION 372
Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?

A. Business Continuity Strategy
B. Index of Disaster-Relevant Information
C. Disaster Invocation Guideline
D. Availability/ ITSCM/ Security Testing Schedule

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
The Business Continuity Strategy is an outline of the approach to ensure the continuity of Vital Business Functions in the case of disaster events. The Business

Continuity Strategy is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy.
Answer: C is incorrect. Disaster Invocation Guideline is a document produced by IT Service Continuity Management with detailed instructions on when and how to invoke the procedure for fighting a disaster. Most importantly, the guideline defines the first step to be taken by the Service Desk after learning that a disaster has occurred. Answer: B is incorrect. Index of Disaster-Relevant Information is a catalogue of all information that is relevant in the event of disasters. This document is maintained and circulated by IT Service Continuity Management to all members of IT staff with responsibilities for fighting disasters.
Answer: D is incorrect. Availability/ ITSCM/ Security Testing Schedule is a schedule for the regular testing of all availability, continuity, and security mechanisms jointly maintained by Availability, IT Service Continuity, and IT Security Management.

QUESTION 373
For which of the following risk management capability maturity levels do the statement given below is true? "Real-time monitoring of risk events and control exceptions exists, as does automation of policy management"

A. Level 3
B. Level 0
C. Level 5
D. Level 2

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
Explanation:
An enterprise's risk management capability maturity level is 5 when real-time monitoring of risk events and control exceptions exists, as does automation of policy management. Answer: B is incorrect. In level 0 of risk management capability maturity model, enterprise does not recognize the importance of considering the risk management or the business impact from IT risk.
Answer: A and D are incorrect. In these levels real-time monitoring of risk events is not done.

QUESTION 374
You are the project manager of the KJH Project and are working with your project team to plan the risk responses. Consider that your project has a budget of $500,000 and is expected to last six months. Within the KJH Project you have identified a risk event that has a probability of .70 and has a cost impact of $350,000. When it comes to creating a risk response for this event what is the risk exposure of the event that must be considered for the cost of the risk response?

A. The risk exposure of the event is $350,000.
B. The risk exposure of the event is $500,000.
C. The risk exposure of the event is $850,000.
D. The risk exposure of the event is $245,000.

Correct Answer: D
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
The risk exposure for this event is found by multiplying the risk impact by the risk probability.
Risk Exposure is a straightforward estimate that gives a numeric value to a risk, enabling different risks to be compared.
Risk Exposure of any given risk = Probability of risk occurring x impact of risk event = 0.70 * 350,000
= 245,000
Answer: A is incorrect. $350,000 is the impact of the risk event. Answer: B is incorrect. $500,000 is the project's budget. Answer: C is incorrect. $850,000 is the project's budget and the risk's impact.

QUESTION 375
Jane, the Director of Sales, contacts you and demands that you add a new feature to the software your project team is creating for the organization. In the meeting she tells you how important the scope change would be. You explain to her that the software is almost finished and adding a change now could cause the deliverable to be late, cost additional funds, and would probably introduce new risks to the project. Jane stands up and says to you, "I am the Director of Sales and this change will happen in the project." And then she leaves the room. What should you do with this verbal demand for a change in the project?

A. Include the change in the project scope immediately.
B. Direct your project team to include the change if they have time.
C. Do not implement the verbal change request.
D. Report Jane to your project sponsor and then include the change.

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
This is a verbal change request, and verbal change requests are never implemented. They introduce risk and cannot be tracked in the project scope. Change requests are requests to expand or reduce the project scope, modify policies, processes, plans, or procedures, modify costs or budgets or revise schedules. These requests for a change can be direct or indirect, externally or internally initiated, and legally or contractually imposed or optional. A Project Manager needs to ensure that only formally documented requested changes are processed and only approved change requests are implemented.
Answer: A is incorrect. Including the verbal change request circumvents the project's change control system.
Answer: D is incorrect. You may want to report Jane to the project sponsor, but you are not obligated to include the verbal change request.
Answer: B is incorrect. Directing the project team to include the change request if they have time is not a valid option. The project manager and the project team will have all of the project team already accounted for so there is no extra time for undocumented, unapproved change requests.

QUESTION 376
You are the risk professional in Bluewell Inc. A risk is identified and enterprise wants to quickly implement control by applying technical solution that deviates from the company's policies. What you should do?

A. Recommend against implementation because it violates the company's policies
B. Recommend revision of the current policy
C. Recommend a risk assessment and subsequent implementation only if residual risk is accepted
D. Conduct a risk assessment and allow or disallow based on the outcome

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
If it is necessary to quickly implement control by applying technical solution that deviates from the company's policies, then risk assessment should be conducted to clarify the risk. It is up to the management to accept the risk or to mitigate it. Answer: D is incorrect. Risk professional can only recommend the risk assessment if the company's policies is violating, but it can only be conducted when the management allows. Answer: A is incorrect. As in this case it is important to mitigate the risk, hence risk professional should once recommend a risk assessment. Though the decision for the conduction of risk assessment in case of violation of company's policy, is taken by management.
Answer: B is incorrect. The recommendation to revise the current policy should not be triggered by a single request.

QUESTION 377
Jane is the project manager of the NHJ Project for his company. He has identified several positive risk events within his project and he thinks these events can save the project time and money. Positive risk events, such as these within the NHJ Project are referred to as?

A. Contingency risks
B. Benefits
C. Residual risk
D. Opportunities

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
A positive risk event is also known as an opportunity. Opportunities within the project to save time and money must be evaluated, analyzed, and responded to. Answer: A is incorrect. A contingency risk is not a valid risk management term. Answer: B is incorrect. Benefits are the good outcomes of a project endeavor. Benefits usually have a cost factor associated with them.
Answer: C is incorrect. Residual risk is the risk that remains after applying controls. It is not feasible to eliminate all risks from an organization. Instead, measures can be taken to reduce risk to an acceptable level. The risk that is left is residual risk.

QUESTION 378

During qualitative risk analysis you want to define the risk urgency assessment. All of the following are indicators of risk priority except for which one?

A. Warning signs
B. Symptoms
C. Risk rating
D. Cost of the project

Correct Answer: D
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The cost of the project is not an indicator of risk urgency. The affect of the risk on the overall cost of the project may be considered, but it is not the best answer. Answer: B is incorrect. Symptoms are an indicator of the risk urgency. Answer: A is incorrect. Warning signs are an indicator of the risk urgency. Answer: C is incorrect. The risk rating can be an indicator of the risk urgency.

QUESTION 379
Which of the following phases is involved in the Data Extraction, Validation, Aggregation and Analysis?

A. Risk response and Risk monitoring
B. Requirements gathering, Data access, Data validation, Data analysis, and Reporting and corrective action
C. Data access and Data validation
D. Risk identification, Risk assessment, Risk response and Risk monitoring

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The basic concepts related to data extraction, validation, aggregation and analysis is important as KRIs often rely on digital information from diverse sources. The phases which are involved in this are:
Requirements gathering: Detailed plan and project's scope is required for monitoring risks. In the case of a monitoring project, this step should involve process owners, data owners, system custodians and other process stakeholders.
Data access: In the data access process, management identifies which data are available and how they can be acquired in a format that can be used for analysis. There are two options for data extraction:
Extracting data directly from the source systems after system owner approval Receiving data extracts from the system custodian (IT) after system owner approval
Direct extraction is preferred, especially since this involves management monitoring its own controls, instead of auditors/third parties monitoring management's controls. If it is not feasible to get direct access, a data access request form should be submitted to the data owners that detail the appropriate data fields to be

extracted. The request should specify the method of delivery for the file.
Data validation: Data validation ensures that extracted data are ready for analysis. One of its important objective is to perform tests examining the data quality to ensure data are valid complete and free of errors. This may also involve making data from different sources suitable for comparative analysis. Following concepts should be considered while validating data:
Ensure the validity, i.e., data match definitions in the table layout Ensure that the data are complete
Ensure that extracted data contain only the data requested Identify missing data, such as gaps in sequence or blank records Identify and confirm the validity of duplicates
Identify the derived values
Check if the data given is reasonable or not
Identify the relationship between table fields
Record, in a transaction or detail table, that the record has no match in a master table Data analysis: Analysis of data involves simple set of steps or complex combination of commands and other functionality. Data analysis is designed in such a way to achieve the stated objectives from the project plan. Although this may be applicable to any monitoring activity, it would be beneficial to consider transferability and scalability. This may include robust documentation, use of software development standards and naming conventions. Reporting and corrective action: According to the requirements of the monitoring objectives and the technology being used, reporting structure and distribution are decided. Reporting procedures indicate to whom outputs from the automated monitoring process are distributed so that they are directed to the right people, in the right format, etc. Similar to the data analysis stage, reporting may also identify areas in which changes to the sensitivity of the reporting parameters or the timing and frequency of the monitoring activity may be required. Answer: D is incorrect. These are the phases that are involved in risk management.

QUESTION 380
Which of the following items is considered as an objective of the three dimensional model within the framework described in COSO ERM?

A. Risk assessment
B. Financial reporting
C. Control environment
D. Monitoring

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
The COSO ERM (Enterprise Risk Management) frame work is a 3-dimentional model. The dimensions and their components include:
Strategic Objectives - includes strategic, operations, reporting, and compliance. Risk Components - includes Internal Environment, Objectives settings, Event identification, Risk assessment, Risk response, Control activities, Information and communication, and monitoring.
Organizational Levels - include subsidiary, business unit, division, and entity-level. The COSO ERM framework contains eight risk components:
Internal Environment
Objective Settings
Event Identification
Risk Assessment

Risk Response
Control Activities
Information and Communication
Monitoring
Section 404 of the Sarbanes-Oley act specifies a three dimensional model- COSO ERM, comprised of Internal control components, Internal control objectives, and organization entities. All the items listed are components except Financial reporting which is an internal control objective.
Answer: C, A, and D are incorrect. They are the Internal control components, not the Internal control objectives.

QUESTION 381
NIST SP 800-53 identifies controls in three primary classes. What are they?

A. Technical, Administrative, and Environmental
B. Preventative, Detective, and Corrective
C. Technical, Operational, and Management
D. Administrative, Technical, and Operational

Correct Answer: C
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
NIST SP 800-53 is used to review security in any organization, that is, in reviewing physical security. The Physical and Environmental Protection family includes 19 different controls. Organizations use these controls for better physical security. These controls are reviewed to determine if they are relevant to a particular organization or not. Many of the controls described include additional references that provide more details on how to implement them. The National Institute of Standards and Technology (NIST) SP 800-53 rev 3 identifies 18 families of controls. It groups these controls into three classes:
Technical
Operational
Management

QUESTION 382
While defining the risk management strategies, what are the major parts to be determined first? Each correct answer represents a part of the solution. Choose two.

A. IT architecture complexity
B. Organizational objectives
C. Risk tolerance
D. Risk assessment criteria

Correct Answer: BC
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
While defining the risk management strategies, risk professional should first identify and analyze the objectives of the organization and the risk tolerance. Once the objectives of enterprise are known, risk professional can detect the possible risks which can occur in accomplishing those objectives. Analyzing the risk tolerance would help in identifying the priorities of risk which is the latter steps in risk management. Hence these two do the basic framework in risk management.
Answer: A is incorrect. IT architecture complexity is related to the risk assessment and not the risk management, as it does much help in evaluating each significant risk identified. Answer: D is incorrect. Risk assessment is one of the various phases that occur while managing risks, which uses quantitative and qualitative approach to evaluate risks. Hence risk assessment criteria is only a part of this framework.

QUESTION 383
Which of the following are external risk factors?
Each correct answer represents a complete solution. Choose three.

A. Geopolitical situation
B. Complexity of the enterprise
C. Market
D. Competition

Correct Answer: AD
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
These three are external risk factors as they lie outside the enterprise's control. Answer: B is incorrect. This includes geographic spread and value chain coverage (for example, in a manufacturing environment). That is why it is internal risk factor.

QUESTION 384
Which of the following is an acceptable method for handling positive project risk?

A. Exploit
B. Avoid
C. Mitigate
D. Transfer

Correct Answer: A
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Exploit is a method for handling positive project risk. Answer: D, B, and C are incorrect. These are all responses which is used for negative risks, and not the positive risk.

QUESTION 385
You are the project manager of GFT project. Your project involves the use of electrical motor. It was stated in its specification that if its temperature would increase to 500 degree Fahrenheit the machine will overheat and have to be shut down for 48 hours. If the machine overheats even once it will delay the project's arrival date. So to prevent this you have decided while creating response that if the temperature of the machine reach 450, the machine will be paused for at least an hour so as to normalize its temperature. This temperature of 450 degree is referred to as?

A. Risk identification
B. Risk trigger
C. Risk event
D. Risk response

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
A risk trigger is a warning sign or condition that a risk event is about to happen. Here the warning temperature is 450 degree Fahrenheit, therefore it is referred as risk trigger. Answer: C is incorrect. Here risk event is 500 degree temperature, as when machine reaches this temperature it should have to be shut-down for 48 hours, which in turn will laid a great impact on the working of project.
Answer: D is incorrect. Risk response here is shutting off of machine when its temperature reaches 450 degree Fahrenheit, so as to prevent the occurring of risk event. Answer: A is incorrect. Risk identification is the process of the identifying the risks. This process identifies the risk events that could affect the project adversely or would act as opportunity.

QUESTION 386
Which of the following decision tree nodes have probability attached to their branches?

A. Root node
B. Event node
C. End node
D. Decision node

Correct Answer: B
Section: Volume B

Explanation

Explanation/Reference:
Explanation:
Event nodes represents the possible uncertain outcomes of a risky decision, with at least two nodes to illustrate the positive and negative range of events. Probabilities are always attached to the branches of event nodes.
Answer: A is incorrect. Root node is the starting node in the decision tree, and it has no branches.
Answer: D is incorrect. It represents the choice available to the decision maker, usually between a risky choice and its non-risky counterpart. As it represents only the choices available to the decision makers, hence probability is not attached to it. Answer: is incorrect. End node represents the outcomes of risk and decisions and probability is not attached to it.

QUESTION 387
Which of the following IS processes provide indirect information? Each correct answer represents a complete solution. Choose three.

A. Post-implementation reviews of program changes
B. Security log monitoring
C. Problem management
D. Recovery testing

Correct Answer: ABC
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Security log monitoring, Post-implementation reviews of program changes, and Problem management provide indirect information. Security log monitoring provide indirect information about certain controls in the security environment, particularly when used to analyze the source of failed access attempts.
Post-implementation reviews of program changes provide indirect information about the effectiveness of internal controls over the development process. Problem management provide indirect information about the effectiveness of several different IS processes that may ultimately be determined to be the source of incidents.
Answer: D is incorrect. Recovery testing is the direct evidence that the redundancy or backup controls work effectively. It doesn't provide any indirect information.

QUESTION 388
You are the risk professional of your enterprise. You need to calculate potential revenue loss if a certain risks occurs. Your enterprise has an electronic (e-commerce) web site that is producing US $1 million of revenue each day, then if a denial of service (DoS) attack occurs that lasts half a day creates how much loss?

A. US $250,000 loss
B. US $500,000 loss
C. US $1 million loss
D. US $100,000 loss

Correct Answer: B
Section: Volume B
Explanation

Explanation/Reference:
Explanation:
Denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name-servers. The term is generally used with regards to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource managementAs the total revenue of the website for the day is $1 million, and due to denial of service attack it is unavailable for half day. Therefore, Revenue loss= $1,000,000/2
= $500,000
Answer: D, A, and C are incorrect. These are wrong answers.

QUESTION 389
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.

Correct Answer: D
Section: Volume A
Explanation

Explanation/Reference:
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 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 390

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.

Correct Answer: C
Section: Volume A
Explanation

Explanation/Reference:
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 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 391
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

Correct Answer: A
Section: Volume A
Explanation

Explanation/Reference:
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.

QUESTION 392
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

Correct Answer: B
Section: Volume A
Explanation

Explanation/Reference:
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 393
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

Correct Answer: AB

Section: Volume A
Explanation

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