CRISC.exam.240q

Number: CRISC
Passing Score: 800
Time Limit: 120 min

CRISC

Certified in Risk and Information Systems Control

Sections

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

4. Volume D

Exam A

QUESTION 1
Which section of the Sarbanes-Oxley Act specifies "Periodic financial reports must be certified by CEO and CFO"?

A. Section 302
B. Section 404C. 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.

Incorrect Answers:
B: Section 404 of the Sarbanes-Oxley Act states that annual assessments of internal controls are the responsibility of management.

C: Section 203 of the Sarbanes-Oxley Act requires audit partners and review partners to rotate off an assignment every five years.

D: Section 409 of the Sarbanes-Oxley Act states that the financial reports must be distributed quickly and currently.

QUESTION 2
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.

Incorrect Answers:
A: 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.

B: Control's design effectiveness is also considered but is latter considered after achieving objectives.

D: Control's operating effectiveness is considered but after its accuracy in objective achievement.

QUESTION 3
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.

Incorrect Answers:

A: Human resources are not affected by fast tracking in most scenarios.

B: Quality control concerns usually are not affected by fast tracking decisions.

C: Costs do not generally increase based on fast tracking decisions.

QUESTION 4
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.

Incorrect Answers:
A: 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.

C: 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.

D: David has not hired a vendor to manage the risk for his project; therefore he is not transferring the risk.

QUESTION 5
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.

Incorrect Answers:
B, C, D: These are also the objectives of the information system control but are not the best answer.

QUESTION 6
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.

Incorrect Answers:
B: Index of Disaster-Relevant Information is a catalog 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.

C: 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.

D: 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 7
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 0C. 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.

Incorrect Answers:
A, D: In these levels real-time monitoring of risk events is not done.

B: 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.

QUESTION 8
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.

Incorrect Answers:
B: CPI is the ratio of earned value to actual cost, i.e., CPI = Earned Value (EV) / Actual Cost (AC).

C: Cost performance index (CPI) is used to calculate performance efficiencies of project and not its schedule.

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

QUESTION 9
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.

Incorrect Answers:
B: Reports that show orders that were rejected for credit limitations provide indirect information that credit checking aspects of the system are working as intended.

C: 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.

D: The lack of any significant differences between perpetual levels and actual levels provides indirect information that its billing controls are operating.

QUESTION 10

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.

Incorrect Answers:
B: This defines the power/interest grid.

C: This defines an influence/impact grid.

D: This defines a power/influence grid.

QUESTION 11

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 12
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.

Incorrect Answers:

B, D: 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.

C: 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 13
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.

Incorrect Answers:
B: Alignment with risk-culture is also one of the factors but is not as important as these two.

C: Risk aware decision is not the factor, but is the result which uses risk appetite information as its input.

QUESTION 14
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.

Incorrect Answers:
A: Risk planning creates the risk management plan and determines how risks will be identified, analyzed, monitored and controlled, and responded to.

C: Risk identification is a process that identifies risk events in the project.

D: Risk analysis helps determine the severity of the risk events, the risks' priority, and the probability and impact of risks.

QUESTION 15
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

Incorrect Answers:
A, C, D: These are not SLEs of this project.

QUESTION 16
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 17
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.

Incorrect Answers:
A: Timely risk reporting is one of the business requirements, but is not the reason behind KRI maintenance.

B: 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.

D: Avoiding risk is a type of risk response. Risk responses are based on KRI reporting.

QUESTION 18
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.

Incorrect Answers:
B, C, D: 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 19
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 subjectmatter expert. Brainstorming is a group creativity technique that also provides other benefits, such as boosting morale, enhancing work enjoyment, and improving team work.

Incorrect Answers:
A: The Delphi technique uses rounds of anonymous surveys to generate a consensus on the identified risks.

B: Expert judgment is not the best answer for this; projects experts generally do the risk identification, in addition to the project team.

D: Checklist analysis uses historical information and information from similar projects within the organization's experience.

QUESTION 20
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:
Explanation:

QUESTION 21
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.

Incorrect Answers:
A: The project plan is not an official PMBOK project management plan.

B: The resource management plan defines the management of project resources, such as project team members, facilities, equipment, and contractors.

C: The project management plan is a comprehensive plan that communicates the intent of the project for all project management knowledge areas.

QUESTION 22
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.

Incorrect Answers:
A: The risk management plan addresses the project management's approach to risk management, risk identification, analysis, response, and control.

B: The project management plan is the overarching plan for the project, not the specifics of the risk responses and risk identification.

C: The risk response plan only addresses the planned risk responses for the identified risk events in the risk register.

QUESTION 23
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.

Incorrect Answers:

B: The act of spending money to reduce a risk probability and impact is known as mitigation.

C: When extra activities are introduced into the project to avoid the risk, this is an example of avoidance.

D: Exploit is a strategy that may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized.

QUESTION 24
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.

Incorrect Answers:
B: 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.

C: 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.

D: It describes how the schedule contingencies will be reported and assessed.

QUESTION 25
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

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

QUESTION 26
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.

Incorrect Answers:
A: The IT strategic plan exists to support the enterprise's strategic plan but is not solely considered while designing information system control.

B: Review of the existing IT environment is also useful and necessary but is not the first step that needs to be undertaken.

D: The present IT budget is just one of the components of the strategic plan.

QUESTION 27
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.

Incorrect Answers:
A: This is the consequence of poor risk communication, not the inhibitor of effective communication.

B: This is the consequence of poor risk communication, not the inhibitor of effective communication.

D: Misalignment between real risk appetite and translation into policies is an inhibitor of effective communication, but is not a prominent as existence of blame culture.

QUESTION 28
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.

Incorrect Answers:
A: These risks are not dismissed; they are still documented on the low priority risk watch list.

B: While these risks may be accepted, they should be documented on the low priority risk watch list. This list will be periodically reviewed and the status of the risks may change.

D: Not every risk demands a risk response, so this choice is incorrect.

QUESTION 29
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.

Incorrect Answers:

B: These controls make effort to reduce the impact of a threat from problems discovered by detective controls. As IDS only detects but not reduce the impact, hence it is not a corrective control.

C: As IDS only detects the problem when it occurs and not prior of its occurrence, it is not preventive control.

D: These controls make efforts to overcome the impact of the incident on the business, hence IDS is not a recovery control.

QUESTION 30
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.

Incorrect Answers:
B: Access Control is the family of controls that helps an organization implement effective access control. They ensure that users have the rights and permissions they need to perform their jobs, and no more. It includes principles such as least privilege and separation of duties.

Audit and accountability family of controls do not help in implementing effective access control.

QUESTION 31
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.

Incorrect Answers:
A, C: Risk appetite level is not relevant in triggering of risk response process. Risk appetite is the amount of risk a company or other entity is willing to accept in pursuit of its mission. This is the responsibility of the board to decide risk appetite of an enterprise. When considering the risk appetite levels for the enterprise, the following two major factors should be taken into account:

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

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

QUESTION 32
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.

Incorrect Answers:
B, C, D: These are not the values of exposure factor for zero assets.

QUESTION 33
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.

Incorrect Answers:
A: Enhancing is a positive risk response that describes actions taken to increase the odds of a risk event to happen.

B: This is an example of a positive risk, but positive is not a risk response.

C: Opportunistic is not a valid risk response.

QUESTION 34
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. A, B, C: These are wrong formulas and are not used in quantitative risk assessment.

QUESTION 35
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.

Incorrect Answers:

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

QUESTION 36
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.

Incorrect Answers:
B: Business process owner is an individual responsible for identifying process requirements, approving process design and managing process performance. He/she is responsible for analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.

C: CIO is the most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. CIO has some responsibility analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.

D: 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 37
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.

Incorrect Answers:
A: Probabilities represent the likelihood of the occurrence of a threat, and this scenario does not describe a probability.

B: Threats are circumstances or events with the potential to cause harm to information resources. This scenario does not describe a threat.

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

QUESTION 38
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.

Incorrect Answers:

A: Penetration testing can identify security vulnerability, but cannot ensure information compliance.

B: Service level monitoring can only identify operational issues in the enterprise's operational environment. It does not play any role in ensuring that outsourced service provider comply with the enterprise's information security policy.

C: Training can increase user awareness of the information security policy, but is less effective than periodic auditing.

QUESTION 39
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.

Incorrect Answers:
A: It addresses costly risk response to a low risk. But here the response is less costly than that of business case to be made.

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

D: This is not risk response prioritization option, instead it is a type of risk that happen with the several of the enterprise's business partners within a very short time frame.

QUESTION 40
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.

Incorrect Answers:
A: While interviewing the firewall administrator may provide a good process overview, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

B: While procedures may provide a good understanding of how the firewall is supposed to be managed, they do not reliably confirm that the firewall configuration complies with the enterprise's security policy.

C: While reviewing the device's log file for recent attacks may provide indirect evidence about the fact that logging is enabled, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

QUESTION 41
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:

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

QUESTION 42
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 plandoes not include responses to risks or triggers. Responses to risks are documented in the risk register as part of the Plan Risk Responses process.

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

QUESTION 43
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 opportunities connected with each possible course of action. This makes them mostly useful for choosing between different strategies, projects, or investment opportunities particularly when the resources are limited. A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.

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

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

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

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

QUESTION 44
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 0C. 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.

Incorrect Answers:
A, C, D: 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 45
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.

Incorrect Answers:
A, C: These two policies are not related to Information system security.

D: 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.

QUESTION 46
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.

Incorrect Answers:
B: Avoidance changes the project plan to avoid the risk altogether.
C: 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.

D: 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 47
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

Incorrect Answers:
A: 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.

C: 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.

D: 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 48
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.

Incorrect Answers:
A, B, C: These all are used to deal with opportunities or positive risks, and not with negative risks.

QUESTION 49
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.

Incorrect Answers:
A: The risk that data cannot be relied on because they are unauthorized, incomplete or inaccurate is termed as integrity risks.

B: The risk of IT projects failing to meet objectives due to lack of accountability and commitment is referring to as project risk ownership.

C: 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.

QUESTION 50
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.

Incorrect Answers:
C, D: 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 51
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 52
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.

Incorrect Answers:
A: You can identify risks before they occur and not after their occurrence.

B: Risks can only happen in the future.

D: Triggers are warning signs and conditions of risk events, but this answer isn't the best choice for this question.

QUESTION 53
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.

Incorrect Answers:
A: 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.

D: 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.

QUESTION 54
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.

Incorrect Answers:
A: The Risk Management Plan defines risk identification, analysis, response, and monitoring.

B: The stakeholder management strategy does not address risk communications.

D: The Resource Management Plan does not define risk communications.

QUESTION 55
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.

Incorrect Answers:
B: Root cause analysis is not an anonymous approach to risk identification.

C: Isolated pilot groups is not a valid risk identification activity.

D: SWOT analysis evaluates the strengths, weaknesses, opportunities, and threats of the project.

QUESTION 56
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.

Incorrect Answers:
B: Threat is the potential cause of unwanted incident.

C: Assets are economic resources that are tangible or intangible, and is capable of being owned or controlled to produce value.

D: Impact is the measure of the financial loss that the threat event may have.

QUESTION 57
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 lowpriority risks, trends in qualitative risk analysis.

Incorrect Answers:
A: Trends in qualitative risk analysis are part of the risk register updates.

C: Risks grouped by categories are part of the risk register updates.

D: Watchlist of low-priority risks is part of the risk register updates.

QUESTION 58
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.

Incorrect Answers:
A: Contagious risks are those risk events that happen with several of the enterprise's business partners within a very short time frame.

B, C: 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 59
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.

Incorrect Answers:
A: 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.

C: A Project Network diagram shows the sequencing and linkage between various project tasks and is not applicable to this question

D: Risk categories are an output of the Perform Qualitative Risk Analysis process and not a tool to complete the process.

QUESTION 60
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.

Incorrect Answers:
A, C, D: The first action required is to create a formal change request, if a change is requested in the project.

QUESTION 61
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.

Incorrect Answers:
B: The risk premium is the difference between the larger expected value of the risk and the smaller certainty equivalent value.

C, D: These are not valid answers.

QUESTION 62
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.

Incorrect Answers:
A: Residual risk is the risk that remains after applying controls. But here in this scenario, risk event has not occurred yet.

C: 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.

D: 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 63
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.

Incorrect Answers:
A, C, D: These are the valid inputs to the perform quantitative risk analysis process.

QUESTION 64
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.

Incorrect Answers:
A: The risk response for these events may be to accept them, but the best answer is to first add them to a watchlist.

C: Risks are not dismissed; they are at least added to a watchlist for monitoring.

D: While the risks may eventually be added to the register, the best answer is to first add them to the watchlist for monitoring.

QUESTION 65
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.

Incorrect Answers:
A: Before the risk events are analyzed they should be documented in the risk register.

B: The risks should first be documented and analyzed.

D: 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.

QUESTION 66
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.

Incorrect Answers:
B: Risk treatment means that action is taken to reduce the frequency and impact of a risk.

C: 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.

D: 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.

QUESTION 67
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.

Incorrect Answers:
C: Business continuity is not considered as risk component within the ERM framework.

QUESTION 68
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 ▪ trends in quantitative
risk analysis

Incorrect Answers:

A, B, D: These subjects are not updated in the risk register as a result of quantitative risk analysis.

QUESTION 69
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.

Incorrect Answers:

A, B, D: These are not plan risk management tools and techniques.

QUESTION 70
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.

Incorrect Answers:
A, B, D: These risks are not such significant as compared to unauthorized access.

QUESTION 71
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.

Incorrect Answers:
A: A residual risk event is similar to a secondary risk, but is often small in probability and impact, so it may just be accepted.

C: Infinitive risk is not a valid project management term.

D: Populated risk event is not a valid project management term.

QUESTION 72
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

Incorrect Answers:
A, C, D: These are not the valid outputs for the qualitative risk analysis process.

QUESTION 73
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.

Incorrect Answers:
B, C, D: Auditing of compliance by external organization is done annually, not quarterly or every three year.

QUESTION 74
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

Incorrect Answers:
A: The risk associated with new system is not meeting the user business needs is business risks, not project risk.
B: This is not direct reason of project risk.

QUESTION 75
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.

Incorrect Answers:
A: The project management plan updates do not create new risks.

B: The organizational process assets updates do not create new risks.

D: The project document updates do not create new risks.

QUESTION 76
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.

Incorrect Answers:
A: Trusted source refers to the commitment of the people designing, implementing, and maintenance of the control towards the security policy.

B: Secure controls refers to the activities ability to protect from exploitation or attack.

D: The separation in design, implementation, and maintenance of controls or countermeasures are refer to as independent. Hence this answer is not valid.

QUESTION 77
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.

Incorrect Answers:
A: This is not a valid statement for reducing bias in the qualitative risk analysis.

B: Positive and negative stakeholders are identified based on their position towards the project goals and objectives, not necessarily risks.

C: Root cause analysis is a good exercise, but it would not determine risk bias.

QUESTION 78
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.

Incorrect Answers:
A: 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.

B: Detective controls simply detect and report on the occurrence of a problems. They identify specific symptoms to potential problems.

C: Compensation controls ensure that normal business operations continue by applying appropriate resource.

QUESTION 79
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 80
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.

Incorrect Answers:
A: Marginal risk causes financial loss in a single line of business and a reduced return on IT investment.

B: It causes minimal impact on a single line of business affecting their ability to deliver services or products.

C: Critical risk causes serious financial losses in more than one line of business with a loss in productivity.

QUESTION 81
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.

Incorrect Answers:
A, B: No such documents as risk alarm and observation list is prepared during risk identification process.

D: 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.

QUESTION 82
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.

Incorrect Answers:
A: 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".

C: 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.

D: 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 83
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.

Incorrect Answers:
A, B, D: 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 84
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 riskaware business decisions, and set the enterprise's risk culture.

Incorrect Answers:

B: 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.

C: 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 85
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

Incorrect Answers:
A: The scenario does not describe risk avoidance. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk.

B: The scenario does not describe the sharing of risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage.

C: The scenario does not describe risk acceptance, Acceptance is a strategy that provides for formal acknowledgment of the existence of a risk and the monitoring of that risk.

QUESTION 86
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.

QUESTION 87
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.

Incorrect Answers:
C: 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 88
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.

Incorrect Answers:
B: 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.

C: 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.

D: Efficiency and effectiveness of controls are not affected by the changes in technology or product, so some measure should be taken.

QUESTION 89
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 90
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.

Incorrect Answers:
A: Benchmarking compares any two items, such as materials, vendors, or resources.

B: 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.

D: Team development describes activities the project manager uses to create a more cohesive and responsive project team.

QUESTION 91
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.

Incorrect Answers:

A, B, C: These all choices vary subjectively.

QUESTION 92
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 opportunities connected with each possible course of action. This makes them mostly useful for choosing between different strategies, projects, or investment opportunities particularly when the resources are limited. A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.

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

B: 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.

D: 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.

QUESTION 93
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.

Incorrect Answers:
B: This includes geographic spread and value chain coverage (for example, in a manufacturing environment). That is why it is internal risk factor.

QUESTION 94
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.

Incorrect Answers:
A, C, D: These are true for risk governance.

QUESTION 95
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.

Incorrect Answers:
A: 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.

C, D: These terms are not applied for the risk that is generated as a result of risk response.

QUESTION 96
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

https://vceplus.com/ 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

Incorrect Answers:
A: 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.

B: 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.

QUESTION 97
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.

Incorrect Answers:
A: Risk identification acts as input of the risk assessment process.

C: This is an output of risk mitigation process, that is, after applying several risk responses.

D: Residual risk is the latter output after appropriate control.

QUESTION 98
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.

Incorrect Answers:
A: Risk mitigation is the latter step after analyzing risk.

B: Risk monitoring is the latter step after risk analysis and risk mitigation.

C: Risk analysis comes under risk management, therefore management is a generalized term, and is not the best answer for this question.

QUESTION 99
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.

Incorrect Answers:
B: It helps in allocating the information concerning risk not only among the decision-makers but also stakeholders.

QUESTION 100
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.

Incorrect Answers:
A: Risk is not unknown, it is uncertain; in addition, the event can affect at least one project objective - not just the project scope.

B: This statement is almost true, but the event does not have to happen within project execution.

C: Risks can affect time, costs, or scope, rather affecting only cost.

QUESTION 101
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.

Incorrect Answers:
A: Role of lag indicators is to ensure that risk after events have occurred is being indicated.

B: 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.

C: Root cause is considered while selecting risk indicator but it does not ensure greater buy-in or ownership.

QUESTION 102
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.

Incorrect Answers:
A: 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.

C: 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.

D: 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.

QUESTION 103
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).

Incorrect Answers:
A: 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.

B: 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.

D: 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.

QUESTION 104
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 noneffective. 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.

Incorrect Answers:
A, C, D: 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 105
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 an agreed-upon basis of evaluating risks. This process should start as soon as project is conceived and should be completed early during project planning.

Incorrect Answers:
A: Risk categories are not defined through the define scope process.

B: Risk categories are not defined through the risk identification process.

D: Risk categories are not defined through the create work breakdown structure process.

QUESTION 106
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.

Incorrect Answers:
B: 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.

C: Lessons learned are not the correct place to document the status of a declined, or approved, change request.

D: The project document updates is not the best choice for this question. It can be placed into the project documents, but the declined changes are part of the change request log.

QUESTION 107
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.

Incorrect Answers:
A, C, D: These all are higher levels of capability maturity model and in this enterprise is mature enough to recognize the importance of risk management.

QUESTION 108
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.

Incorrect Answers:
B: 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.

C, D: These are not sufficient for producing detailed result.

QUESTION 109
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'

Incorrect Answers:
A, D: These two are the methods of analyzing risk, but not specifically for high-impact risk types. Hence is not the best answer.

B: 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 110
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.

Incorrect Answers:
A: Communication with business process stakeholders is done so as to identify the business objectives, but it does not help in identifying impacts.

C: Compliance-oriented gap analysis will only identify the gaps in compliance to current requirements and will not identify impacts to business objectives.

D: Mapping of compliance requirements to policies and procedures will identify only the way the compliance is achieved but not the business impact.

QUESTION 111

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.

Incorrect Answers:
A: The Risk management plan is an input to the risk qualitative analysis process.

B: The project scope statement is needed to help with qualitative risk analysis.

C: The risk register can help Wendy to perform qualitative risk analysis.

QUESTION 112
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.

Incorrect Answers:
A, B, C: These are the valid inputs to the Risk Monitoring and Controlling Process.

QUESTION 113
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.

Incorrect Answers:
A: 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.

B: 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.

D: The process improvement plan aims to improve the project's processes regardless of scope changes.

QUESTION 114
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.

Incorrect Answers:
B: Process integrity is confirmed within the system, it dose not need monitoring.

C: Configuration settings are generally compared against predefined values and not based on the correlation between multiple sources.

D: System changes are compared from a previous state to the current state, it dose not correlate information from multiple sources.

QUESTION 115
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

Incorrect Answers:
D: Project management plan is not a security plan, but a plan which describes the implementation of the project.

QUESTION 116
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 IT 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.

Incorrect Answers:
A: 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 117

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 base 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 in the report any internal controls or changes to those internal controls which have been implemented since they were evaluated.

Incorrect Answers:
A: The signing officer has evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report, not at the time of the report.

QUESTION 118
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.

Incorrect Answers:
A: The configuration management system controls and documents changes to the project's product

C: The change log documents approved changes in the project scope.

D: The scope change control system controls changes that are permitted to the project scope.

QUESTION 119
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.

Incorrect Answers:
A: Risk management provides an approach for individuals and groups to make a decision on how to deal with potentially harmful situations

B: 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.

C: 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.

QUESTION 120

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.

Incorrect Answers:
B: 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.

C: Chief financial officer is the most senior official of the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks.

D: 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 121
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.

Incorrect Answers:
C: 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 122
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.

Incorrect Answers:
B: 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.

C: The contractual relationship won't change with the vendor as far as project risks are concerned.

D: The project scope statement is changed as part of the scope approval that has already happened.

QUESTION 123
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 either 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.

Incorrect Answers:
D: Risk management is planned latter in project development process, and not during initialization.

QUESTION 124
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.

Incorrect Answers:
A, B, C: These factors in combination contribute to the overall financial impact, i.e., financial losses incurred by affected business units.

QUESTION 125
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.

Incorrect Answers:
A: Detective controls simply detect and report on the occurrence of problems. They identify specific symptoms to potential problems.

C: 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.

D: Scope creep refers to small undocumented changes to the project scope.

QUESTION 126
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.

Incorrect Answers:
A: Configuration management defines the management, control, and documentation of the features and functions of the project's product.

C: Risk analysis is not responsible for reviewing the change aspects for the entire project.

D: The project change control system defines the workflow and approval process for proposed changes to the project scope, time, cost, and contracts.

QUESTION 127
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

Incorrect Answers:
A, C: 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 128
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.

Incorrect Answers:
A: 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.

D: 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 129
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.

Incorrect Answers:
A: Risk factors are expressed in terms of high/medium/low in qualitative analysis, and not in quantitative analysis.

QUESTION 130
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.

Incorrect Answers:
A: Risk probability distributions do not typically interact with the bias towards risks in new resources.

B: Risk probability distributions are not likely to be used with risk probability and impact matrices.

D: Risk probability distributions are not likely the risk identification.

QUESTION 131
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.

Incorrect Answers:
A, B: There are no such concepts existing in manipulating risk level.

D: 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.

QUESTION 132
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.
B: 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.

Incorrect Answers:
A: 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.

C: 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.

QUESTION 133
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.

Incorrect Answers:
A, B, D: 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 134
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.

Incorrect Answers:
B: This is not a 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.

C: 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.

QUESTION 135
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

Incorrect Answers:
A: Data gathering and representation technique is a tool and technique for the quantitative risk analysis process.

B: Expert judgment is a tool and technique for the quantitative risk analysis process.

C: Quantitative risk analysis and modeling techniques is a tool and technique for the quantitative risk analysis process.

QUESTION 136
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.

Incorrect Answers:
A: 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.

B: This is not the valid answer.

C: Type of market in which the enterprise is operating do not affect the selection of KPIs.

QUESTION 137
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.

Incorrect Answers:
A: 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.

C: This isn't an example of exploiting. Exploiting is an action to take advantage of a positive risk response that will happen.

D: Crashing does add costs, but in this instance, crashing is an example of the positive risk response of enhancing.

QUESTION 138
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.

Incorrect Answers:
A: Exploit risk response is used for positive risk or opportunity, not for negative risk.

B: This risk response does require a change request, in some instances, but it's the avoidance risk response and not just a change request.

D: 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.

QUESTION 139
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 140
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.

Incorrect Answers:
B: 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.

C: 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.

D: 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 141
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 142
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.

Incorrect Answers:
B: 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 143
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

Incorrect Answers:
A, B, C: These are not valid number of communication channels for the given scenario.

QUESTION 144
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

Incorrect Answers:
B: 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 145
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.

Incorrect Answers:

A: It evaluates the internal control structure of process of functional area.

B: Audits that assesses the correctness of financial statements is called financial audit.

D: They are the IS audits with specific intent to examine areas, such as processes, services, or technologies, usually by third party auditors.

QUESTION 146
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.

Incorrect Answers:
A: Risk management happens throughout the project as does project planning.

B: Milestones are good times to do reviews, but risk management should happen frequently.

C: This answer would only be correct if the project has a status meeting just once per month in the project.

QUESTION 147
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.

Incorrect Answers:
B, C, D: Stakeholder identification, Assessment information, and Stakeholder classification should be included in the stakeholder register.

QUESTION 148
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 twentyeight 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 149
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.

Incorrect Answers:
A: 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.

B: 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.

D: Enhancing is a positive risk response that aims to increase the probability and/or impact of the risk event.

QUESTION 150
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.

Incorrect Answers:
A: Risk cannot be completely eliminated from the enterprise.

C: This is not a valid answer.

D: Mitigation of risk is itself the risk response process, not the reason behind this.

QUESTION 151
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.

Incorrect Answers:
A: An intrusion detection system does not protect against phishing attacks since phishing attacks usually do not have a particular pattern or unique signature.

B: 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.

D: 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.

QUESTION 152
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.

Incorrect Answers:
A: GLBA is not used for handling health care information.

C: SOX designed to hold executives and board members personally responsible for financial data.

D: FISMA ensures protection of data of federal agencies.

QUESTION 153
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 154
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 155
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: ACD

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 156
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

Incorrect Answers:
A: Reporting risks are those occurrences which prevent accurate and timely reporting.

C: 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.

D: 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.

QUESTION 157
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.

Incorrect Answers:
B: The risk event created by the application of risk response is called secondary risk.

C: A risk event that is generated due to errors or omission in the project work is not necessarily pure risk.

D: This in not valid definition of pure risk.

QUESTION 158
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

Incorrect Answers:
A, B ,C: These are incorrect choices as only 4 risk response are available to deal with negative risks.

QUESTION 159
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

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

QUESTION 160
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.

Incorrect Answers:
A: The IT strategic plan exists to support the enterprise's strategic plan but is not solely considered while designing information system control.

B: Review of the existing IT environment is also useful and necessary but is not the first step that needs to be undertaken.

D: The present IT budget is just one of the components of the strategic plan.

QUESTION 161
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 lackof 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.

Incorrect Answers:
A: This is the consequence of poor risk communication, not the inhibitor of effective communication.

B: This is the consequence of poor risk communication, not the inhibitor of effective communication.

D: Misalignment between real risk appetite and translation into policies is an inhibitor of effective communication, but is not a prominent as existence of blame culture.

QUESTION 162
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.

Incorrect Answers:
A: These risks are not dismissed; they are still documented on the low priority risk watch list.

B: While these risks may be accepted, they should be documented on the low priority risk watch list. This list will be periodically reviewed and the status of the risks may change.

D: Not every risk demands a risk response, so this choice is incorrect.

QUESTION 163
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.

Incorrect Answers:
B: These controls make effort to reduce the impact of a threat from problems discovered by detective controls. As IDS only detects but not reduce the impact, hence it is not a corrective control.

C: As IDS only detects the problem when it occurs and not prior of its occurrence, it is not preventive control.

D: These controls make efforts to overcome the impact of the incident on the business, hence IDS is not a recovery control.

QUESTION 164
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.

Incorrect Answers:
B: Access Control is the family of controls that helps an organization implement effective access control. They ensure that users have the rights and permissions they need to perform their jobs, and no more. It includes principles such as least privilege and separation of duties. Audit and accountability family of controls do not help in implementing effective access control.

QUESTION 165
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.

Incorrect Answers:
A, C: Risk appetite level is not relevant in triggering of risk response process. Risk appetite is the amount of risk a company or other entity is willing to accept in pursuit of its mission. This is the responsibility of the board to decide risk appetite of an enterprise. When considering the risk appetite levels for the enterprise, the following two major factors should be taken into account:
- The enterprise's objective capacity to absorb loss, e.g., financial loss, reputation damage, etc.
- The culture towards risk taking-cautious or aggressive. In other words, the amount of loss the enterprise wants to accept in pursue of its objective fulfillment.

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

QUESTION 166
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.

Incorrect Answers:
B, C, D: These are not the values of exposure factor for zero assets.

QUESTION 167
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.

Incorrect Answers:
A: Enhancing is a positive risk response that describes actions taken to increase the odds of a risk event to happen.

B: This is an example of a positive risk, but positive is not a risk response.

C: Opportunistic is not a valid risk response.

QUESTION 168
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. A, B, C: These are wrong formulas and are not used in quantitative risk assessment.

QUESTION 169
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.

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

QUESTION 170
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.

Incorrect Answers:
B: Business process owner is an individual responsible for identifying process requirements, approving process design and managing process performance. He/she is responsible for analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.

C: CIO is the most senior official of the enterprise who is accountable for IT advocacy; aligning IT and business strategies; and planning, resourcing and managing the delivery of IT services and information and the deployment of associated human resources. CIO has some responsibility analyzing risks, maintaining risk profile, and risk-aware decisions but is not accounted for them.

D: 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 171
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.

Incorrect Answers:
A: Probabilities represent the likelihood of the occurrence of a threat, and this scenario does not describe a probability.

B: Threats are circumstances or events with the potential to cause harm to information resources. This scenario does not describe a threat.

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

QUESTION 172
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.

Incorrect Answers:
A: Penetration testing can identify security vulnerability, but cannot ensure information compliance.

B: Service level monitoring can only identify operational issues in the enterprise's operational environment. It does not play any role in ensuring that outsourced service provider comply with the enterprise's information security policy.

C: Training can increase user awareness of the information security policy, but is less effective than periodic auditing.

QUESTION 173
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.

Incorrect Answers:
A: It addresses costly risk response to a low risk. But here the response is less costly than that of business case to be made.

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

D: This is not risk response prioritization option, instead it is a type of risk that happen with the several of the enterprise's business partners within a very short time frame.

QUESTION 174
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.

Incorrect Answers:
A: While interviewing the firewall administrator may provide a good process overview, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

B: While procedures may provide a good understanding of how the firewall is supposed to be managed, they do not reliably confirm that the firewall configuration complies with the enterprise's security policy.

C: While reviewing the device's log file for recent attacks may provide indirect evidence about the fact that logging is enabled, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

QUESTION 175
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:
Incorrect Answers:
A, B, D: Productivity, quality and customer service are used for evaluating critical service factor of any particular project.

QUESTION 176
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.

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

QUESTION 177
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 opportunities connected with each possible course of action. This makes them mostly useful for choosing between different strategies, projects, or investment opportunities particularly when the resources are limited. A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.

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

B: Cause-and-effect analysis is used for exposing risk factors and not an effective one in risk response planning. This analysis involves the use of predictive or diagnostic analytical tool for exploring the root causes or factors that contribute to positive or negative effects or outcomes.

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

QUESTION 178
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.

Incorrect Answers:
B: 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.

C: Reducing risk to a level too small to measure is not practical and is often cost-prohibitive.

D: Reducing risks to a specific return ignores the qualitative aspects of the risk which should also be considered.

QUESTION 179
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.

Incorrect Answers:
B, C, D: Data owners are not responsible for intrusion detection, platform security or antivirus controls.
These are the responsibilities of data custodians.

QUESTION 180
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.

Incorrect Answers:
A, C: These two policies are not related to Information system security.

D: 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.

QUESTION 181
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.

Incorrect Answers:
B: Avoidance changes the project plan to avoid the risk altogether.

C: 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.

D: 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 182
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.

Incorrect Answers:
B: This is the process of numerically analyzing the effect of identified risks on overall project objectives.

C: This is the process of determining which risks may affect the project and documenting their characteristics.

D: This is the process of prioritizing risks for further analysis or action by accessing and combining their probability of occurrence and impact.

QUESTION 183
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.

Incorrect Answers:
A: It is not an input for Plan risk management process.

QUESTION 184
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.

Incorrect Answers:
A: 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.

B: 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.

D: 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 185
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.

Incorrect Answers:
A: Risk reduction efforts can focus on either avoiding the frequency of the risk or reducing the impact of a risk.

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

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

QUESTION 186
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.

Incorrect Answers:
A: 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.

B: 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.

D: 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.

QUESTION 187
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.

Incorrect Answers:
A: The system users are responsible for utilizing the system properly and following procedures, but they do not own the risk.
C: The IT director manages the IT systems on behalf of the business owners.
D: The risk management department determines and reports on level of risk, but does not own the risk. Risk is owned by senior management.

QUESTION 188

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.

Incorrect Answers:
A: Configuration management controls and documents changes to the features and functions of the product scope.
B: Scope change control focuses on the processes to allow changes to enter the project scope.
C: Risk monitoring and control is not part of the change control system, so this choice is not valid.

QUESTION 189
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.

Incorrect Answers:
C, E: 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 190
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.

Incorrect Answers:
A, B, D: These are not the valid definitions of the policy.

QUESTION 191

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.

Incorrect Answers:
A: Status of enterprise's risk can be determined only after risk monitoring.
B: Appropriate control can only be determined as the result of risk assessment, not through residual risk.

QUESTION 192
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.

Incorrect Answers:
B: Risk response plans are implemented as part of the monitoring and controlling process group.

C: Risk response plans are not implemented as part of project planning.

D: Risk response plans are not implemented as part of project execution.

QUESTION 193
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.

Incorrect Answers:
A, B: 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.
C: SLE, ARO and ALE are used in quantitative risk assessment.

QUESTION 194
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.

Incorrect Answers:
A: 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

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

D: 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.

QUESTION 195
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 reserveC. 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.

Incorrect Answers:
A: The risk response plan is based on the risk responses, not the risk probability-impact matrix.

C: The risk responses are needed but this chart doesn't help the project manager to create them.

D: This chart is created as part of quantitative analysis.

QUESTION 196
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.

Incorrect Answers:
B: Tools are not the parts of SWOT analysis.

QUESTION 197
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:
▪ 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.

Incorrect Answers:

A, C, D: These all phases occur in IS monitoring and maintenance process after prioritizing risks.

QUESTION 198
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.

Incorrect Answers:

A: Root cause analysis examines causal factors for events within the project.

B: Influence diagramming techniques examines the relationships between things and events within the project.

D: Assumptions analysis does not use four pre-defined perspectives for review.

QUESTION 199
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.

Incorrect Answers:
A: It does not provide direct information as there is no information about the propriety of cutoff.

C, D: These are not the types of information.

QUESTION 200
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 2C. 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.

Incorrect Answers:

A: Enterprise having risk management capability maturity level 0 takes business decisions without considering risk credential information.

B: 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 201
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.

Incorrect Answers:
B: 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.

C: While the project manager shouldn't be the only person to identify the risk events, this isn't the best answer.

D: 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.

QUESTION 202
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.

Incorrect Answers:
A: Frameworks are generally accepted, business-process-oriented structures that establish a common language and enable repeatable business processes.

B: These are legal rules underneath which project has to be.

D: 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.

QUESTION 203
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

Incorrect Answers:
D: There is no such model exists in risk management process.

B: 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.

C: Fishbone diagrams or Ishikawa diagrams shows the relationships between the causes and effects of problems.

QUESTION 204
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.

Incorrect Answers:
B, C, D: 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 205
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.

Incorrect Answers:
A, C, D: As explained in above section preventive control and prevention is preferred over detection and recovery, hence these are less preferred way.

QUESTION 206
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.

Incorrect Answers:
B: 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.

C: Requirements of the project is being defined after conducting feasibility study.

D: This is latter phase in project development process.

QUESTION 207
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 2C. 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.

Incorrect Answers:
A: In level 3 of risk management capability maturity model, local tolerances drive the enterprise risk tolerance.

B: In level 2 of risk management capability maturity model, risk tolerance is set locally and may be difficult to aggregate.

C: In level 4 of risk management capability maturity model, business risk tolerance is reflected by enterprise policies and standards reflect.

QUESTION 208
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.

Incorrect Answers:
A: Control management charts are not the place where risk events are recorded.

B: This is a risk event and should be recorded in the risk register.

D: Risks that have a low probability and a low impact may go on the low-level risk watch-list.

QUESTION 209
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.

Incorrect Answers:
A: 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.

B: 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.

C: Transference is a negative risk response where the project manager hires a third party to own the risk event.

QUESTION 210
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

Incorrect Answers:
A, C, D CCTV is a physical control.

QUESTION 211
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 life cycle. 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.

Incorrect Answers:
B: The cost management plan defines the estimating, budgeting, and control of the project's cost.

C: While the cost management plan does define the cost change control system, this is not the best answer for this

D: This is not a valid statement. The cost management plan is an input to the quantitative risk analysis process.

QUESTION 212
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.

Incorrect Answers:
B: The stakeholder register is a listing of stakeholder information and communication requirements.

C: The influence/impact grid charts is based on the stakeholders involvement and ability to effect changes to the project's planning and execution.

D: The salience model groups the stakeholders based on their power, urgency, and legitimacy in the project.

QUESTION 213
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.

Incorrect Answers:
B: 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 question.

C: Lessons learned are not the correct place to document the status of a declined, or approved, change request.

D: The project document updates is not the best choice for this to be fleshed into the project documents, but the declined changes are part of the change request log.

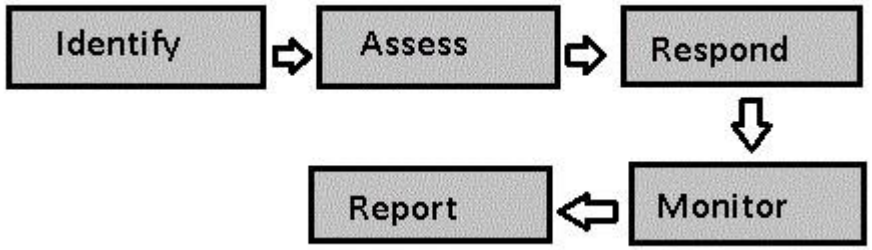
QUESTION 214
Which of the following comes under phases of risk management?

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 215
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 216
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 217
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.

Incorrect Answers:
A: 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.

B, C: These are options are not valid.

QUESTION 218
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.

Incorrect Answers:
B: This is the responsibility of Change advisory board.

D: 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 219
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.

Incorrect Answers:
A: Natural disaster can be a short-term, but it is not the best answer.

B: Natural disaster can be a long-term, but it is not the best answer.

D: Natural disaster can be of large impact depending upon its nature, but it is not the best answer.

QUESTION 220
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.

Incorrect Answers:
A: It controls accounting operations, including safeguarding assets and financial records.

B: Detective control simply detects and reports on the occurrence of an error, omission or malicious act.

D: It focuses on day-to-day operations, functions, and activities. It also ensures that all the organization's objectives are being accomplished.

QUESTION 221

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.

Incorrect Answers:
A: Key risk Indicators (KRIs) only provide insights into potential risks that may exist or be realized within a concept or capability that they monitor.

B: Capability maturity models (CMMs) assess the maturity of a concept or capability and do not provide insights into operational effectiveness.

D: Metric thresholds are decision or action points that are enacted when a KPI or KRI reports a specific value or set of values.

QUESTION 222
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.

Incorrect Answers:
B: Auditors identify threats and vulnerability not only in the IT but the whole enterprise as well.

QUESTION 223
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.

Incorrect Answers:
A: The cost change control system is responsible for reviewing and controlling changes to the project costs.

C: 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.

D: Integrated change control examines the affect of a proposed change on the project as a whole.

QUESTION 224
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.

Incorrect Answers:

B: 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.

D: This is not a valid answer.

QUESTION 225
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.

Incorrect Answers:
A: 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.

B: Since the likelihood determines the size of the loss, hence both elements must be considered in the calculation.

C: A risk analysis would not normally consider the benchmark of similar companies as providing relevant information other than for comparison purposes.

QUESTION 226
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.

Incorrect Answers:
A, B, C: 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 227
You work as a project manager for TechSoft Inc. You are working with the project stakeholders on the qualitative risk analysis process in your project. You have used all the tools to the qualitative risk analysis process in your project. Which of the following techniques is NOT used as a 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.

Incorrect Answers:
A, C, D: 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 228
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.

Incorrect Answers:
A, B, C: Integrity, availability, and confidentiality of data are also important, but these three in combination comes under reliability itself.

QUESTION 229
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.

Incorrect Answers:
A: Sharing is a positive risk response. Note that sharing may also have contractual obligations, sometimes called teaming agreements.

C: Mitigation is a negative risk response used to lower the probability and/or impact of a risk event.

D: Exploiting is a positive risk response and not a negative response and doesn't have contractual obligations.

QUESTION 230
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.

Incorrect Answers:
B: 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.

C: 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.

D: 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 231
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.

Incorrect Answers:
A: 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.

C: 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.

D: 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.

QUESTION 232
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.

Incorrect Answers:
A: Notification of failure does not determine control strength, hence this option is not correct.

B: The type of control, like preventive or detective, does not help determine control effectiveness.

C: Reliability is not an indication of control strength; weak controls can be highly reliable, even if they do not meet the control objective.

QUESTION 233
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.

Incorrect Answers:
A, B, C: These all are less significant than identifying controls.

QUESTION 234
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

Incorrect Answers:
C: Risk register is updated after applying appropriate risk response and at the time of risk event occurrence.

QUESTION 235
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

Incorrect Answers:
B: 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 236
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.

Incorrect Answers:

B, D: Identification and authentication, and audit and accountability control are technical class of controls.

QUESTION 237
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

Incorrect Answers:
C: Risk appetite and risk tolerance are considered when applying various risk responses.

QUESTION 238
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 239
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:
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

Incorrect Answers:
A, B, C: These are the earlier phases in policy development process.

QUESTION 240
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.

Incorrect Answers:
B: 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.

C: 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.

D: Risk response is the action taken to reduce the risk event occurrence. Hence here risk response is shutting off of machine.