Examskey Isaca CRISC exam demo product is here for you to test the quality of the product. This Isaca CRISC demo also ensures that we have this product ready unlike most companies, which arrange the product for you as you order. These CRISC exam questions are prepared by Isaca subject matter specialists. Hence these are most accurate version of the CRISC exam questions that you can get in the market.

We also offer bundle discount packages for every Isaca certification track, so you can buy all related exam questions in one convenient bundle. And for corporate clients we also offer bundles for Isaca certification exams at huge discount.

Check out our CRISC Exam Page and Isaca Certification Page for more details of these bundle packages.
Question: 1

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

A. Identify Risks  
B. Qualitative Risk Analysis  
C. Quantitative Risk Analysis  
D. Plan Risk Management

Answer: B

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

Answer: C is incorr

Quantitative analysis is the use of numerical and statistical techniques rather than the analysis of verbal material for analyzing risks. Some of the quantitative methods of risk analysis are:
- Internal loss method
- External data analysis
- Business process modeling (BPM) and simulation
- Statistical process control (SPC)

Answer: A is incorr

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

Answer: D is incorr

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

Question: 2
Which of the following characteristics of baseline represents specification that is used to identify approved requirements in baseline modeling?

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

**Answer: B**

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

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

**Question: 3**

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

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

**Answer: D, B, and A**

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

**Question: 4**

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

A. SOX  
B. GLBA  
C. HIPAA  
D. FISMA

**Answer: C**

**Explanation:**
HIPAA handles health care information of an organization. The Health Insurance Portability and Accountability Act (HIPAA) were introduced in 1996. It ensures that health information data is protected. Before HIPAA, personal medical information was often available to anyone. Security to protect the data was lax, and the data was often misused. If your organization handles health information, HIPAA applies. HIPAA defines health information as any data that is created or received by health care providers, health plans, public health authorities, employers, life insurers, schools or universities, and health care clearinghouses. HIPAA defines any data that is related to the health of an individual, including past/present/future health, physical/mental health, and past/present/future payments for health care. Creating a HIPAA compliance plan involves following phases:

- **Assessment:** An assessment helps in identifying whether organization is covered by HIPAA. If it is, then further requirement is to identify what data is needed to protect.
- **Risk analysis:** A risk analysis helps to identify the risks. In this phase, analyzing method of handling data of organization is done.
- **Plan creation:** After identifying the risks, plan is created. This plan includes methods to reduce the risk.
- **Plan implementation:** In this plan is being implemented.
- **Continuous monitoring:** Security in depth requires continuous monitoring. Monitor regulations for changes. Monitor risks for changes.
- **Monitor the plan to ensure it is still used.**
- **Assessment:** Regular reviews are conducted to ensure that the organization remains in compliance.

**Answer: A is incorr**

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

**Answer: B is incorr**

GLBA is not used for handling health care information.
FISMA ensures protection of data of federal agencies.

**Question: 5**

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

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

**Answer: C**

**Explanation:**
Exploit response is one of the strategies to negate risks or threats that appear in a project. This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Exploiting a risk event provides opportunities for positive impact on a project. Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.

- 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.

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

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

**Question: 6**
You are the project manager of the NHQ project in Bluewell Inc. The project has an asset valued at $200,000 and is subjected to an exposure factor of 45 percent. If the annual rate of occurrence of loss in this project is once a month, then what will be the Annual Loss Expectancy (ALE) of the project?

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

**Answer: D**

**Explanation:**
The ALE of this project will be $ 108,000.

Single Loss Expectancy is a term related to Quantitative Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows:

\[
SLE = \text{Asset value} \times \text{Exposure factor}
\]

Therefore,

\[
SLE = 200,000 \times 0.45
\]

\[= 90,000\]

As the loss is occurring once every month, therefore ARO is 12. Now ALE can be calculated as follows:

\[
ALE = SLE \times ARO
\]

\[= 90,000 \times 12\]

\[= $ 108,000\]

**Question: 7**

Which of the following is NOT true for Key Risk Indicators?

A. The complete set of KRIs should also balance indicators for risk, root causes and business impact.  
B. They help avoid having to manage and report on an excessively large number of risk indicators  
C. They are monitored annually  
D. They are selected as the prime monitoring indicators for the enterprise

**Answer: C**

**Explanation:**
They are monitored on regular basis as they indicate high probability and high impact risks. As risks change over time, hence KRIs should also be monitored regularly for its effectiveness on these changing risks.
are incorrect. These all are true for KRIs. Key Risk Indicators are the prime monitoring indicators of the enterprise. KRIs are highly relevant and possess a high probability of predicting or indicating important risk. KRIs help in avoiding excessively large number of risk indicators to manage and report that a large enterprise may have. The complete set of KRIs should also balance indicators for risk, root causes and business impact, so as to indicate the risk and its impact completely.

Question: 8

You work as a project manager for SoftTech Inc. You are working with the project stakeholders to begin the qualitative risk analysis process. Which of the following inputs will be needed for the qualitative risk analysis process in your project? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: D, B, and C

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

Answer: A is incorr

ect. The cost management plan is the input to the perform quantitative risk analysis process.

Question: 9

You have identified several risks in your project. You have opted for risk mitigation in order to respond to identified risk. Which of the following ensures that risk mitigation method that you have chosen is effective?

A. Reduction in the frequency of a threat
B. Minimization of inherent risk
C. Reduction in the impact of a threat
D. Minimization of residual risk

**Answer: B**

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

**Answer: D is incorr**

**Answer: A is incorr**

**Answer: C is incorr**

**Question: 10**

Which of the following methods involves the use of predictive or diagnostic analytical tool for exposing risk factors?

A. Fault tree analysis
B. Scenario analysis
C. Sensitivity analysis
D. Cause and effect analysis

**Answer: D**

**Explanation:**
Cause-and-effect analysis involves the use of predictive or diagnostic analytical tool for exploring the root causes or factors that contribute to positive or negative effects or outcomes. These tools also help in identifying potential risk.

**Answer: C is incorr**
Sensitivity analysis is the quantitative risk analysis technique that:
Assist in determination of risk factors that have the most potential impact
Examines the extent to which the uncertainty of each element affects the object under consideration when all other uncertain elements are held at their baseline values

**Answer: A is incorr**

Fault tree analysis (FIA) is a technique that provides a systematic description of the combination of possible occurrences in a system, which can result in an undesirable outcome. It combines hardware failures and human failures.

**Answer: B is incorr**

This analysis is not a method for exposing risk factors. It is used for analyzing scenarios.

**Question: 11**

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 team and the project manager can work together to assign risk ownership.
C. So that the project manager can identify the risk owners for the risks within the project and the needed risk responses.
D. So that the project manager isn't the only person identifying the risk events within the project.

**Answer: A**

Explanation:
The best answer to include the project team members is that they'll need to develop a sense of ownership for the risks and associated risk responsibilities.

**Answer: D is incorr**

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

**Answer: B is incorr**

The reason to include the project team is that the project team needs to develop a sense of ownership for the risks and associated risk responsibilities, not to assign risk ownership.

**Answer: C is incorr**
ect. The reason to include the project team is that the project team needs to develop a sense of ownership for the risks and associated risk responsibilities, not to assign risk ownership and risk responses at this point.

**Question: 12**

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. the vendor database to user accounts.
C. access requests to user accounts.
D. user accounts to access requests.

**Answer: D**

Explanation:
Tying user accounts to access requests confirms that all existing accounts have been approved. Hence, the effectiveness of the system access management process can be accounted.

**Answer: C is incorr**

t. Tying access requests to user accounts confirms that all access requests have been processed; however, the test does not consider user accounts that have been established without the supporting access request.

**Answer: A is incorr**

t. Tying user accounts to human resources (HR) records confirms whether user accounts are uniquely tied to employees, not accounts for the effectiveness of the system access management process.

**Answer: B is incorr**

t. Tying vendor records to user accounts may confirm valid accounts on an e-commerce application, but it does not consider user accounts that have been established without the supporting access request.

**Question: 13**

You are the administrator of your enterprise. You have to prevent unauthorized access to an enterprise's information. Which of the following control you would use?

A. User authentication
B. User identification
C. User authorization
D. User accountability

Answer: A

Explanation:
Authentication verifies the user’s identity and the right to access information according to the access rules. Hence it prevents unauthorized access to an enterprise’s information.

Answer: D is incorr

Answer: B is incorr

Answer: C is incorr

Question: 14

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. Expert judgment
B. Quantitative risk analysis and modeling techniques
C. Organizational process assets
D. Data gathering and representation techniques

Answer: C

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

**Answer:** D is incorr

Data gathering and representation technique is a tool and technique for the quantitative risk analysis process.

**Answer:** B is incorr

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

**Answer:** A is incorr

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

**Question: 15**

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

**Answer:** B

Explanation:
Key Performance Indicators is a set of measures that a company or industry uses to measure and/or compare performance in terms of meeting their strategic and operational goals. KPIs vary with company to company, depending on their priorities or performance criteria. A company must establish its strategic and operational goals and then choose their KPIs which can best reflect those goals. For example, if a software company's goal is to have the fastest growth in its industry, its main performance indicator may be the measure of its annual revenue growth.

**Answer:** D is incorr

This is not the valid answer.

**Answer:** A is incorr
Determination of size and complexity of the enterprise is the selection criteria of the KRI, not KPI. KPI does not have any relevancy with size and complexity of the enterprise.

**Answer:** C is incorr

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

**Question: 16**

Which of the following serve as the authorization for a project to begin?

A. Approval of project management plan  
B. Approval of risk management document  
C. Approval of a risk response document  
D. Approval of a project request document

**Answer:** D

**Explanation:**
Approval of a project initiation document (PID) or a project request document (PRD) is the authorization for a project to begin.

**Answer:** B is incorr

effect. Risk management document is being prepared later after the project initiation, during the risk management plan. It has no scope during project initialization.

**Answer:** C is incorr

effect. Risk response document comes under risk management process, hence the latter phase in project development process.

**Answer:** A is incorr

effect. Project management plan is being made after the project is being authorized.

**Question: 17**

You work as the project manager for www.company.com Inc. The project on which you are working has several risks that will affect several stakeholder requirements. Which project management plan will define who will be available to share information on the project risks?

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

Answer: B

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 Management Plan identifies and defines the roles of persons concerned with the project. It includes a matrix known as the communication matrix to map the communication requirements of the project.

Answer: C is incorr

ect. The stakeholder management strategy does not address risk communications.

Answer: A is incorr


Answer: D is incorr


Question: 18

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

Answer: A

Explanation:
Senior management is responsible for the acceptance and mitigation of all risk. Hence they will also own the risk to an information system that supports a critical business process.
Answer: D is incorr

The IT director manages the IT systems on behalf of the business owners.

Answer: C is incorr

The risk management department determines and reports on level of risk, but does not own the risk. Risk is owned by senior management.

Answer: B is incorr

The system users are responsible for utilizing the system properly and following procedures, but they do not own the risk.

Question: 19

Which of the following statements is NOT true for risk management plan?

A. The risk management plan includes a description of the responses to risks and triggers.
B. The risk management plan is an input to all the remaining risk-planning processes.
C. The risk management plan is an output of the Plan Risk Management process.
D. The risk management plan includes thresholds, scoring and interpretation methods, responsible parties, and budgets.

Answer: A

Explanation:
The risk management plan details how risk management processes will be implemented, monitored, and controlled throughout the life of the project. The risk management plan does not include responses to risks or triggers. Responses to risks are documented in the risk register as part of the Plan Risk Responses process.

Answer: C, D, and B

are incorrect. These statements are true for risk management plan. The risk management is the result of Plan Risk Management process and do act as input for the remaining risk-planning process. It also includes thresholds, scoring and interpretation methods, responsible parties, and budgets.

Question: 20

Which of the following comes under phases of risk management?

A. Identify risk
B. Developing risk

Answer: A, B

Identify risk and Developing risk are under phases of risk management.
C. Assessing risk  
D. Prioritization of risk  
E. Monitoring risk

Answer: A, C, D, and E

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: 21

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

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

Answer: A

Explanation:
The Communications Management Plan will direct John on the information to be communicated, when to communicate, and how to communicate with external stakeholders. The Communications
Management Plan aims to define the communication necessities for the project and how the information will be circulated. The Communications Management Plan sets the communication structure for the project. This structure provides guidance for communication throughout the project's life and is updated as communication needs change. The Communication Managements Plan identifies and defines the roles of persons concerned with the project. It includes a matrix known as the communication matrix to map the communication requirements of the project.

**Answer: C is incorr**

The Risk Management Plan defines how risks will be identified, analyzed, responded to, and controlled throughout the project.

**Answer: B is incorr**

The Risk Response Plan identifies how risks will be responded to.

**Answer: D is incorr**

The Project Management Plan is the parent of all subsidiary management plans and it is not the most accurate choice for this Question.

**Question: 22**

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

A. Quality management plan  
B. Stakeholder register  
C. Cost management plan  
D. Procurement management plan

**Answer: D**

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

**Question: 23**
You are an experienced Project Manager that has been entrusted with a project to develop a machine which produces auto components. You have completed identification of possible risks that could impact the project, prioritize, and planning responses to those risks. After your project has been underway for 3 months, your project sponsor has asked for an evaluation of how your risk response plans were faring. Which of the following would provide you that information?

A. Risk Reassessment
B. Risk Audit
C. Variance Analysis
D. Reserve Analysis

**Answer: B**

**Explanation:**
Risk Audits examine and document the effectiveness of risk responses in dealing with identified risks and their root causes, as well as the effectiveness of the risk management processes.

**Answer: A is incorr**

Risk Reassessment is the process of identification of new risks, reassessment of current risks, and the closing of the risks that are outdated; not what the Sponsor is asking.

**Answer: C is incorr**

Variance Analysis compares planned results to the actual results, and in this context measures the trends in project execution.

**Answer: D is incorr**

Reserve analysis compares the amount of contingency reserve remaining to the amount of risk remaining at any time in the project in order to determine if the remaining reserve is adequate.

**Question: 24**

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

**Answer: B**
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.

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

**Answer:** A is incorrect.

Audit and Accountability control helps an organization implement an effective audit program. It provides details on how to determine what to audit. It provides details on how to protect the audit logs. It also includes information on using audit logs for non-repudiation.

**Explanation:**
Audit and Accountability control helps an organization implement an effective audit program. It provides details on how to determine what to audit. It provides details on how to protect the audit logs. It also includes information on using audit logs for non-repudiation.

**Answer:** C is incorrect.

Identification and Authentication control cover different practices to identify and authenticate users. Each user should be uniquely identified. In other words, each user has one account. This account is only used by one user. Similarly, device identifiers uniquely identify devices on the network.

**Explanation:**
Identification and Authentication control cover different practices to identify and authenticate users. Each user should be uniquely identified. In other words, each user has one account. This account is only used by one user. Similarly, device identifiers uniquely identify devices on the network.

**Answer:** D is incorrect.

System and Communications protection control is a large group of controls that cover many aspects of protecting systems and communication channels. Denial of service protection and boundary protection controls are included. Transmission integrity and confidentiality controls are also included.

**Question: 25**

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

**Answer:** B

**Explanation:**
Risk register is a document that contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning. Risk register is developed along with all processes of the risk management from Plan Risk Management through Monitor and Control Risks.

**Answer:** D is incorrect.
addresses quality control (QC), quality assurance (QA), and continuous process improvement for the project. Based on the requirement of the project, the quality management plan may be formal or informal, highly detailed or broadly framed.

**Answer: C is incorr**

Risk management plan includes roles and responsibilities, risk analysis definitions, timing for reviews, and risk threshold. The Plan Risk Responses process takes input from risk management plan and risk register to define the risk response.

**Answer: A is incorr**

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.
THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CRISC Exam Questions With Answers.

http://www.examskey.com/CRISC.html

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Download Free Product Demo From:

http://www.examskey.com/CRISC.html

Money Back Guarantee

Check Out Our Customer Testimonials

http://vimeo.com/102521210