QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

CRISC Dumps
CRISC Braindumps
CRISC Real Questions
CRISC Practice Test
CRISC dumps free

ISACA

CRISC

Certified in Risk and Information Systems Control

QUESTION: 391
Jane, the Director of Sales, contacts you and demands that you add a new feature to the software your project team is creating for the organization. In the meeting she tells you how important the scope change would be. You explain to her that the software is almost finished and adding a change now could cause the deliverable to be late, cost additional funds, and would probably introduce new risks to the project. Jane stands up and says to you, "I am the Director of Sales and this change will happen in the project." And then she leaves the room. What should you do with this verbal demand for a change in the project?

A. Include the change in the project scope immediately.
B. Direct your project team to include the change if they have time.
C. Do not implement the verbal change request.
D. Report Jane to your project sponsor and then include the change.

Answer: C

Explanation:
This is a verbal change request, and verbal change requests are never implemented. They introduce risk and cannot be tracked in the project scope. Change requests are requests to expand or reduce the project scope, modify policies, processes, plans, or procedures, modify costs or budgets or revise schedules. These requests for a change can be direct or indirect, externally or internally initiated, and legally or contractually imposed or optional. A Project Manager needs to ensure that only formally documented requested changes are processed and only approved change requests are implemented. Answer. A is incorrect. Including the verbal change request circumvents the project's change control system. Answer. D is incorrect. You may want to report Jane to the project sponsor, but you are not obligated to include the verbal change request. Answer. B is incorrect. Directing the project team to include the change request if they have time is not a valid option. The project manager and the project team will have all of the project team already accounted for so there is no extra time for undocumented, unapproved change requests.

QUESTION: 392
You are the risk professional in Bluewell Inc. A risk is identified and enterprise wants to quickly implement control by applying technical solution that deviates from the company's policies. What you should do?

A. Recommend against implementation because it violates the company's policies
B. Recommend revision of the current policy
C. Recommend a risk assessment and subsequent implementation only if residual risk is accepted
D. Conduct a risk assessment and allow or disallow based on the outcome

Answer: C

Explanation:
If it is necessary to quickly implement control by applying technical solution that deviates from the company's policies, then risk assessment should be conducted to clarify the risk. It is up to the management to accept the risk or to mitigate it. Answer. D is incorrect. Risk professional can only recommend the risk assessment if the company's policies is violating, but it can only be conducted when the management allows. Answer. A is incorrect. As in this case it is important to mitigate the risk, hence risk professional should once recommend a risk assessment. Though the decision for the conduction of risk assessment in case of violation of company's policy, is taken by management. Answer. B is incorrect. The recommendation to revise the current policy should not be triggered by a single request.

QUESTION: 393
Jane is the project manager of the NHJ Project for his company. He has identified several positive risk events within his project and he thinks these events can save the project time and money. Positive risk events, such as these within the NHJ Project are referred to as?

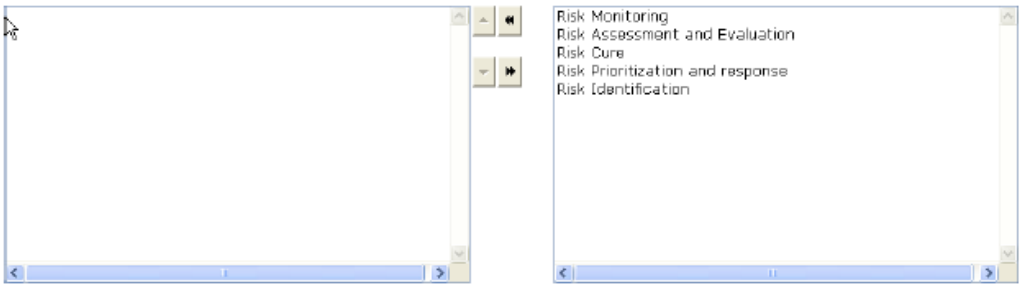
A. Contingency risks
B. Benefits
C. Residual risk
D. Opportunities

Answer: D

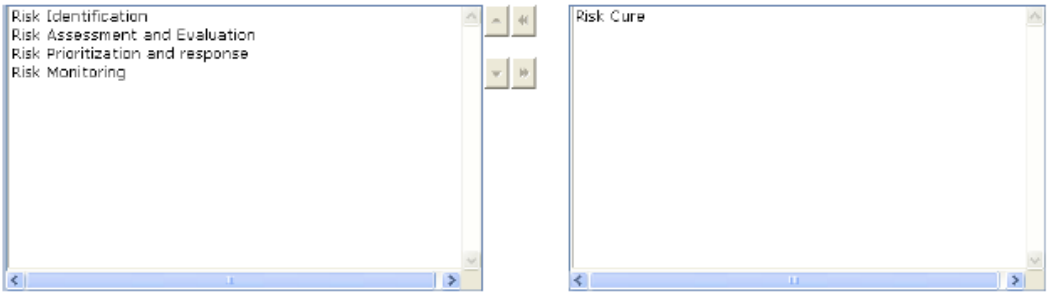
Explanation:
A positive risk event is also known as an opportunity. Opportunities within the project to save time and money must be evaluated, analyzed, and responded to. Answer. A is incorrect. A contingency risk is not a valid risk management term.

Answer. B is incorrect. Benefits are the good outcomes of a project endeavor. Benefits usually have a cost factor associated with them. Answer. C is incorrect. Residual risk is the risk that remains after applying controls. It is not feasible to eliminate all risks from an organization. Instead, measures can be taken to reduce risk to an acceptable level. The risk that is left is residual risk.

QUESTION: 394
Arrange the following in the sequence as they occur in the different Phases of Risk Management.

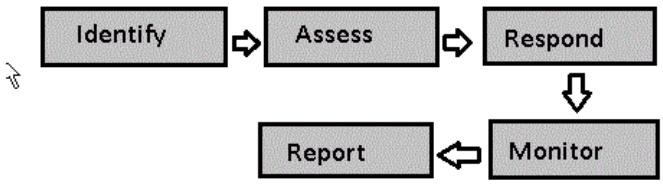


Answer:



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: 395
Which of the following phases is involved in the Data Extraction, Validation, Aggregation and Analysis ?

A. Risk response and Risk monitoring
B. Requirements gathering, Data access, Data validation, Data analysis, and Reporting and corrective action
C. Data access and Data validation
D. Risk identification, Risk assessment, Risk response and Risk monitoring

Answer: B

Explanation:
The basic concepts related to data extraction, validation, aggregation and analysis is important as KRIs often rely on digital information from diverse sources. The phases which are involved in this are: Requirements gathering: Detailed plan and project's scope is required for monitoring risks. In the case of a monitoring

project, this step should involve process owners, data owners, system custodians and other process stakeholders.
Data access: In the data access process, management identifies which data are available and how they can be acquired in a format that can be used for analysis. There are two options for data extraction:
Extracting data directly from the source systems after system owner approval Receiving data extracts from the system custodian (IT) after system owner approval Direct extraction is preferred, especially since this involves management monitoring its own controls, instead of auditors/third parties monitoring management's controls. If it is not feasible to get direct access, a data access request form should be submitted to the data owners that detail the appropriate data fields to be extracted. The request should specify the method of delivery for the file.
Data validation: Data validation ensures that extracted data are ready for analysis. One of its important objective is to perform tests examining the data quality to ensure data are valid complete and free of errors. This may also involve making data from different sources suitable for comparative analysis. Following concepts should be considered while validating data:
Ensure the validity, i.e., data match definitions in the table layout
Ensure that the data are complete
Ensure that extracted data contain only the data requested Identify missing data, such as gaps in sequence or blank records Identify and confirm the validity of duplicates
Identify the derived values
Check if the data given is reasonable or not
Identify the relationship between table fields
Record, in a transaction or detail table, that the record has no match in a master table
Data analysis: Analysis of data involves simple set of steps or complex combination of commands and other functionality. Data analysis is designed in such a way to achieve the stated objectives from the project plan. Although this may be applicable to any monitoring activity, it would be beneficial to consider transferability and scalability. This may include robust documentation, use of software development standards and naming conventions.
Reporting and corrective action: According to the requirements of the monitoring objectives and the technology being used, reporting structure and distribution are decided. Reporting procedures indicate to whom outputs from the automated monitoring process are distributed so that they are directed to the right people, in the right format, etc. Similar to the data analysis stage, reporting may also identify areas in which changes to the sensitivity of the reporting parameters or the timing and frequency of the
monitoring activity may be required. Answer. D is incorrect. These are the phases that are involved in risk management.

QUESTION: 396
Which of the following items is considered as an objective of the three dimensional model within the framework described in COSO ERM?

A. Risk assessment
B. Financial reporting
C. Control environment
D. Monitoring

Answer: B

Explanation:
The COSO ERM (Enterprise Risk Management) frame work is a 3-dimentional model. The dimensions and their components include:
Strategic Objectives - includes strategic, operations, reporting, and compliance.
Risk Components - includes Internal Environment, Objectives settings, Event identification, Risk assessment, Risk response, Control
activities, Information and communication, and monitoring.
Organizational Levels - include subsidiary, business unit, division, and entity-level.
The COSO ERM framework contains eight risk components:
Internal Environment Objective Settings Event Identification Risk Assessment
Risk Response
Control Activities
Information and Communication
Monitoring
Section 404 of the Sarbanes-Oley act specifies a three dimensional model- COSO ERM, comprised of Internal control components, Internal control objectives, and organization entities. All the items listed are components except Financial reporting which is an internal control objective. Answer. C, A, and D are incorrect. They are the Internal control components, not the Internal control objectives.

QUESTION: 397
NIST SP 800-53 identifies controls in three primary classes. What are they?

A. Technical, Administrative, and Environmental
B. Preventative, Detective, and Corrective
C. Technical, Operational, and Management
D. Administrative, Technical, and Operational

Answer: C

Explanation:
NIST SP 800-53 is used to review security in any organization, that is, in reviewing physical security. The Physical and Environmental Protection family includes 19 different controls. Organizations use these controls for better physical security. These controls are reviewed to determine if they are relevant to a particular organization or not. Many of the controls described include additional references that provide
more details on how to implement them. The National Institute of Standards and Technology (NIST) SP 800-53 rev 3 identifies 18 families of controls. It groups these controls into three classes:
Technical Operational Management

QUESTION: 398
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

Answer: B, C

Explanation:
While defining the risk management strategies, risk professional should first identify and analyze the objectives of the organization and the risk tolerance. Once the objectives of enterprise are known, risk professional can detect the possible risks which can occur in accomplishing those objectives. Analyzing the risk tolerance would help in identifying the priorities of risk which is the latter steps in risk management. Hence these two do the basic framework in risk management. Answer. A is incorrect. IT architecture complexity is related to the risk assessment and not the risk management, as it does much help in evaluating each significant risk identified. Answer. D is incorrect. Risk assessment is one of the various phases that occur while managing risks, which uses quantitative and qualitative approach to evaluate risks. Hence risk assessment criteria is only a part of this framework.

QUESTION: 399
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

Answer: D, B, C

Explanation:
As quantitative analysis is data driven, it: Allows data classification and counting.
Allows statistical models to be constructed, which help in explaining what is being observed. Generalizes findings for a larger population and direct comparisons between two different sets of data or observations.
Produces statistically reliable results.
Allows discovery of phenomena which are likely to be genuine and merely occurs by chance. Answer. is incorrect. Risk factors are expressed in terms of high/medium/low in qualitative analysis, and not in quantitative analysis.

QUESTION: 400
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

Answer: C

Explanation:
Risk probability distributions are likely to be utilized in uncertain values, such as time and cost estimates for a project. Answer. D is incorrect. Risk probability

distributions are not likely the risk identification. Answer. B is incorrect. Risk probability distributions are not likely to be used with risk probability and impact matrices. Answer. A is incorrect. Risk probability distributions do not typically interact with the bias towards risks in new resources.