DUMPSARENA

Certified in Risk and Information Systems Control

Isaca CRISC

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1799

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, New Update	710
Topic 2, Volume A	100
Topic 3, Volume B	100
Topic 4, Volume C	99
Topic 5, Volume D	790
Total	1799

QUESTION NO: 1

When reviewing a business continuity plan (BCP), which of the following would be the MOST significant deficiency?

A. BCP is often tested using the walkthrough method

B. BCP testing is not in conjunction with the disaster recovery plan (DRP)

C. Each business location has separate, inconsistent BCPs

D. Recovery time objectives (RTOs) do not meet business requirements

ANSWER: B

QUESTION NO: 2

A vulnerability assessment of a vendor-supplied solution has revealed that the software is susceptible to cross-site scripting and SQL injection attacks. Which of the following will BEST mitigate this issue?

A. Require the software vendor to remediate the vulnerabilities.

B. Approve exception to allow the software to continue operating.

C. Monitor the databases for abnormal activity.

D. Accept the risk and let the vendor run the software as is.

ANSWER: A

QUESTION NO: 3

What are the various outputs of risk response?

A. Risk Priority Number

B. Residual risk

C. Risk register updates

D. Project management plan and Project document updates

E. Risk-related contract decisions

ANSWER: C D E

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 acts 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 NO: 4

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 stakeholder does, not just what it says.

ANSWER: A C D

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 NO: 5

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

ANSWER: A B D

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 NO: 6

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: B C D

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 NO: 7

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

ANSWER: A D

Explanation:

The board of directors and senior management has the responsibility to set up the risk governance process, establish and maintain a common risk view, make risk-aware business decisions, and set the enterprise's risk culture.

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 NO: 8

The BEST indication that risk management is effective is when risk has been reduced to meet:

A. risk appetite

B. risk capacity

C. risk levels

D. risk budgets

ANSWER: A

QUESTION NO: 9

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 three.)

A. Quality management plan

B. Schedule management plan

C. Cost management plan

D. Project scope statement

ANSWER: B C D

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 NO: 10

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

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

A. Obscure risk

B. Risk factors

C. Risk analysis

D. Risk event

ANSWER: B

Explanation:

Risk factors are those features that influence the likelihood and/or business impact of risk scenarios. They have heavy influences on probability and impact of risk scenarios. They should be taken into account during every risk analysis, when likelihood and impact are assessed.

Incorrect Answers:

A: 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

C: 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.

D: A risk event represents the situation where you have a risk that only occurs with a certain probability and where the risk itself is represented by a specified distribution.

QUESTION NO: 11

Which of the following is the GREATEST benefit when enterprise risk management (ERM) provides oversight of IT risk management?

A. Prioritizing internal departments that provide service to customers

B. Ensuring the IT budget and resources focus on risk management

C. Ensuring senior management's primary focus is on the impact of identified risk

D. Aligning IT with short-term and long-term goals of the organization

ANSWER: D

QUESTION NO: 12

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

ANSWER: A C D

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 NO: 13

Which of the following issues found during the review of a newly created disaster recovery plan (DRP) should be of MOST concern?

A. Some critical business applications are not included in the plan

B. Several recovery activities will be outsourced

C. The plan is not based on an internationally recognized framework

D. The chief information security officer (CISO) has not approved the plan

ANSWER: A

QUESTION NO: 14

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

ANSWER: B

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 NO: 15

Which of the following come under the phases of risk identification and evaluation?

Each correct answer represents a complete solution. (Choose three.)

A. Maintain a risk profile

B. Collecting data

C. Analyzing risk

D. Applying controls

ANSWER: A B C

Explanation:

Risk identification is the process of determining which risks may affect the project. It also documents risks' characteristics.

Following are high-level phases that are involved in risk identification and evaluation:

- Collecting data- Involves collecting data on the business environment, types of events, risk categories, risk scenarios, etc., to identify relevant data to enable effective risk identification, analysis and reporting.

- Analyzing risk- Involves analyzing risk to develop useful information which is used while taking risk-decisions. Risk-decisions take into account the business relevance of risk factors.

- Maintain a risk profile- Requires maintaining an up-to-date and complete inventory of known threats and their attributes (e.g., expected likelihood, potential impact, and disposition), IT resources, capabilities, and controls as understood in the context of business products, services and processes to effectively monitor risk over time.

Incorrect Answers:

D: It comes under risk management process, and not in risk identification and evaluation process.

QUESTION NO: 16

Qualitative risk assessment uses which of the following terms for evaluating risk level?

Each correct answer represents a part of the solution. (Choose two.)

A. Impact

B. Annual rate of occurrence

C. Probability

D. Single loss expectancy

ANSWER: A C

Explanation:

Unlike the quantitative risk assessment, qualitative risk assessment does not assign dollar values. Rather, it determines risk's level based on the probability and impact of a risk. These values are determined by gathering the opinions of experts.

- Probability- establishing the likelihood of occurrence and reoccurrence of specific risks, independently, and combined. The risk occurs when a threat exploits vulnerability. Scaling is done to define the probability that a risk will occur. The scale can be based on word values such as Low, Medium, or High. Percentage can also be assigned to these words, like 10% to low and 90% to high.

- Impact- Impact is used to identify the magnitude of identified risks. The risk leads to some type of loss. However, instead of quantifying the loss as a dollar value, an impact assessment could use words such as Low, Medium, or High. Impact is expressed as a relative value. For example, low could be 10, medium could be 50, and high could be 100. Risk level = Probability * Impact

Incorrect Answers:

B, D: These are used for calculating Annual loss expectancy (ALE) in quantitative risk assessment. Formula is given as follows: ALE= SLE * ARO

QUESTION NO: 17

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

A. Assess whether existing controls meet the regulation

B. Update the existing security privacy policy

C. Meet with stakeholders to decide how to comply

D. Analyze the key risk in the compliance process

ANSWER: A

Explanation:

When a new regulation for safeguarding information processed by a specific type of transaction is being identified by the IT manager, then the immediate step would be to understand the impact and requirements of this new regulation. This includes assessing how the enterprise will comply with the regulation and to what extent the existing control structure supports the compliance process. After that manager should then assess any existing gaps.

Incorrect Answers:

B, C, D: These choices are appropriate as well as important, but are subsequent steps after understanding and gap assessment.

QUESTION NO: 18

A service provider is managing a client's servers. During an audit of the service, a noncompliant control is discovered that will not be resolved before the next audit because the client cannot afford the downtime required to correct the issue. The service provider's MOST appropriate action would be to:

A. develop a risk remediation plan overriding the client's decision

B. make a note for this item in the next audit explaining the situation

C. insist that the remediation occur for the benefit of other customers

D. ask the client to document the formal risk acceptance for the provider

ANSWER: D

QUESTION NO: 19

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

A. Section 302

B. Section 404

C. Section 203

D. Section 409

ANSWER: A

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 NO: 20

Which of the following come under the management class of controls?

Each correct answer represents a complete solution. (Choose two.)

A. Risk assessment control

B. Audit and accountability control

C. Program management control

D. Identification and authentication control

ANSWER: A C

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.