CAP Q&As

CAP - Certified Authorization Professional

Pass ISC CAP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/cap.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

QUESTION 1

Which of the following is NOT an objective of the security program?

A. Security organization

B. Security plan

C. Security education

D. Information classification

Correct Answer: B

QUESTION 2

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

A. Risk avoidance

B. Mitigation-ready project management

C. Risk utility function

D. Risk-reward mentality

Correct Answer: C

QUESTION 3

Which of the following assessment methods involves observing or conducting the operation of physical devices?

A. Interview

B. Deviation

C. Examination

D. Testing

Correct Answer: D

QUESTION 4

Which of the following statements correctly describes DIACAP residual risk?

A. It is the remaining risk to the information system after risk palliation has occurred.

B. It is a process of security authorization.

C. It is the technical implementation of the security design.

D. It is used to validate the information system.

Correct Answer: A

QUESTION 5

Which of the following assessment methodologies defines a six-step technical security evaluation?

A. OCTAVE

B. FITSAF

C. DITSCAP

D. FIPS 102

Correct Answer: D

QUESTION 6

During which of the following processes, probability and impact matrix is prepared?

A. Plan Risk Responses

B. Perform Quantitative Risk Analysis

C. Perform Qualitative Risk Analysis

D. Monitoring and Control Risks

Correct Answer: C

QUESTION 7

Your project has several risks that may cause serious financial impact should they happen. 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 for 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. Quantitative analysis

B. Risk response plan

C. Contingency reserve

D. Risk response

Correct Answer: C

QUESTION 8

Which of the following RMF phases identifies key threats and vulnerabilities that could compromise the confidentiality, integrity, and availability of the institutional critical assets?

A. Phase 2

B. Phase 1

C. Phase 3

D. Phase 0

Correct Answer: B

QUESTION 9

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

A. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.

B. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.

C. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.

D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

Correct Answer: D

QUESTION 10

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance

(IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight

areas of IA defined by DoD?

Each correct answer represents a complete solution. Choose all that apply.

A. VI Vulnerability and Incident Management

B. DC Security Design and Configuration

C. EC Enclave and Computing Environment

D. Information systems acquisition, development, and maintenance

Correct Answer: ABC

QUESTION 11

Which of the following DITSCAP CandA phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?

A. Phase 3

B. Phase 1

C. Phase 2

D. Phase 4

Correct Answer: C

QUESTION 12

In which of the following phases do the system security plan update and the Plan of Action and Milestones (POAM) update take place?

A. Continuous Monitoring Phase

B. Accreditation Phase

C. Preparation Phase

D. DITSCAP Phase

Correct Answer: A

QUESTION 13

Which of the following individuals is responsible for configuration management and control task?

A. Authorizing official

B. Information system owner

C. Chief information officer

D. Common control provider

Correct Answer: B

QUESTION 14

During qualitative risk analysis you want to define the risk urgency assessment. All of the following are indicators of risk priority except for which one?

A. Symptoms

B. Cost of the project

C. Warning signs

D. Risk rating

Correct Answer: B

QUESTION 15

Which of the following is NOT a type of penetration test?

A. Cursory test

B. Partial-knowledge test

C. Zero-knowledge test

D. Full knowledge test

Correct Answer: A