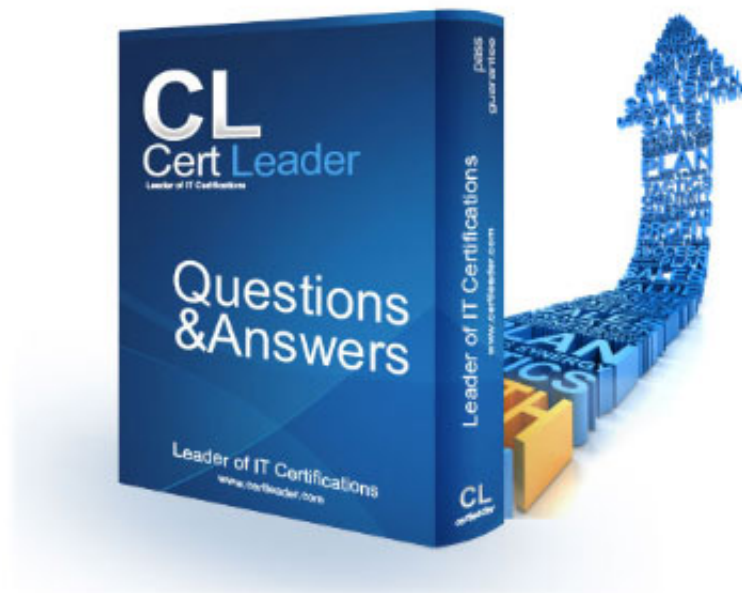


CAP - ISC2 CAP Certified Authorization Professional

<http://www.certleader.com/CAP-dumps.html>



1. Which of the following are the goals of risk management?

Each correct answer represents a complete solution. Choose three.

- A. Finding an economic balance between the impact of the risk and the cost of the countermeasure
- B. Identifying the risk
- C. Assessing the impact of potential threats
- D. Identifying the accused

Answer: ABC

2. In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

- A. Full operational test
- B. Penetration test
- C. Paper test
- D. Walk-through test

Answer: B

3. You are the project manager of the GHG project. You are preparing for the quantitative risk analysis process. You are using organizational process assets to help you complete the quantitative risk analysis process. Which one of the following is NOT a valid reason to utilize organizational process assets as a part of the quantitative risk analysis process?

- A. You will use organizational process assets for studies of similar projects by risk specialists.
- B. You will use organizational process assets to determine costs of all risks events within the current project.
- C. You will use organizational process assets for information from prior similar projects.
- D. You will use organizational process assets for risk databases that may be available from industry sources.

Answer: B

4. Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

- A. SSAA
- B. FIPS

C. FITSAF

D. TCSEC

Answer: A

5. Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

A. Acceptance

B. Mitigation

C. Avoidance

D. Transference

Answer: C

6. Which of the following statements is true about residual risks?

A. It is a weakness or lack of safeguard that can be exploited by a threat.

B. It can be considered as an indicator of threats coupled with vulnerability.

C. It is the probabilistic risk after implementing all security measures.

D. It is the probabilistic risk before implementing all security measures.

Answer: C

7. 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. Risk register

B. Risk management plan

C. Project charter

D. Quality management plan

Answer: A

8. 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. Cost management plan
- B. Quality management plan
- C. Procurement management plan
- D. Stakeholder register

Answer: C

9. Mary is the project manager of the HGH Project for her company. She and her project team have agreed that if the vendor is late by more than ten days they will cancel the order and hire the NBG Company to fulfill the order. The NBG Company can guarantee orders within three days, but the costs of their products are significantly more expensive than the current vendor. What type of a response strategy is this?

- A. External risk response
- B. Internal risk management strategy
- C. Contingent response strategy
- D. Expert judgment

Answer: C

10. Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

- A. FITSAF
- B. TCSEC
- C. FIPS
- D. SSAA

Answer: B

11. Your project uses a piece of equipment that if the temperature of the machine goes above 450 degree Fahrenheit the machine will overheat and have to be shut down for 48 hours. Should this machine overheat even once it will delay the project's end date. You work with your project to create a response that should the temperature of the machine reach 430, the machine will be paused for at least an hour to cool it down. The temperature of 430 is called what?

- A. Risk identification
- B. Risk response
- C. Risk trigger
- D. Risk event

Answer: C

12. 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. DC Security Design & Configuration
- B. VI Vulnerability and Incident Management
- C. EC Enclave and Computing Environment
- D. Information systems acquisition, development, and maintenance

Answer: ABC

13. Which of the following is an Information Assurance (IA) model that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation?

- A. Parkerian Hexad
- B. Capability Maturity Model (CMM)
- C. Classic information security model
- D. Five Pillars model

Answer: D

14. You work as a project manager for BlueWell Inc. Your project is running late and you must respond to the risk. Which risk response can you choose that will also cause you to update the human resource management plan?

- A. Teaming agreements
- B. Crashing the project
- C. Transference

D. Fast tracking the project

Answer: B

15. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 2

B. Level 3

C. Level 5

D. Level 4

E. Level 1

Answer: B

16. You are the project manager for your company and a new change request has been approved for your project. This change request, however, has introduced several new risks to the project. You have communicated these risk events and the project stakeholders understand the possible effects these risks could have on your project. You elect to create a mitigation response for the identified risk events. Where will you record the mitigation response?

A. Risk register

B. Risk log

C. Risk management plan

D. Project management plan

Answer: A

17. Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

A. Continuity of Operations Plan

B. Disaster recovery plan

C. Contingency plan

D. Business continuity plan

Answer: C

18. The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase?

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

- A. System development
- B. Certification analysis
- C. Registration
- D. Assessment of the Analysis Results
- E. Configuring refinement of the SSAA

Answer: ABDE

19. ISO 17799 has two parts. The first part is an implementation guide with guidelines on how to build a comprehensive information security infrastructure and the second part is an auditing guide based on requirements that must be met for an organization to be deemed compliant with ISO 17799. What are the ISO 17799 domains?

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

- A. Information security policy for the organization
- B. Personnel security
- C. Business continuity management
- D. System architecture management
- E. System development and maintenance

Answer: ABCE

20. Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation?

Each correct answer represents a complete solution. Choose two.

- A. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
- B. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
- C. Certification is the official management decision given by a senior agency official to authorize operation of an information system.

D. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.

Answer: AD

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CAP Exam with Our Prep Materials Via below:

<http://www.certleader.com/CAP-dumps.html>