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.pass4itsure.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 statements about Discretionary Access Control List (DACL) is true?

A. It is a rule list containing access control entries.

B. It specifies whether an audit activity should be performed when an object attempts to access a resource.

C. It is a unique number that identifies a user, group,and computer account.

D. It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.

Correct Answer: D

QUESTION 2

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

A. FITSAF

B. FIPS 102

C. OCTAVE

D. DITSCAP

Correct Answer: B

QUESTION 3

You work as a project manager for BlueWell Inc. You are working with your team members on the risk responses in the project. Which risk response will likely cause a project to use the procurement processes?

A. Acceptance

B. Mitigation

C. Exploiting

D. Sharing

Correct Answer: D

QUESTION 4

Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event?

A. Corrective action

B. Technical performance measurement

C. Risk audit

D. Earned value management

Correct Answer: A

QUESTION 5

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 6

In which of the following Risk Management Framework (RMF) phases is strategic risk assessment planning performed?

A. Phase 0

B. Phase 1

C. Phase 2

D. Phase 3

Correct Answer: A

QUESTION 7

Which of the following is NOT a responsibility of a data owner?

A. Maintaining and protecting data

B. Ensuring that the necessary security controls are in place

C. Delegating responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian

D. Approving access requests

Correct Answer: A

QUESTION 8

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

A. Safeguards

B. Preventive controls

C. Detective controls

D. Corrective controls

Correct Answer: D

QUESTION 9

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

A. Security plan

B. Security education

C. Security organization

D. Information classification

Correct Answer: A

QUESTION 10

Security Test and Evaluation (STandE) is a component of risk assessment. It is useful in discovering system vulnerabilities. For what purposes is STandE used? Each correct answer represents a complete solution. Choose all that apply.

A. To implement the design of system architecture

B. To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy

C. To assess the degree of consistency between the system documentation and its implement ation

D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

Correct Answer: BCD

QUESTION 11

Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the international

information security standards? Each correct answer represents a complete solution. Choose all that apply.

A. Human resources security

B. Organization of information security

C. Risk assessment and treatment

D. AU audit and accountability

Correct Answer: ABC

QUESTION 12

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores,

transmits, or processes unclassified or classified information since December 1997. What phases are

identified by DIACAP?

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

A. Accreditation

B. Identification

C. System Definition

D. Verification

E. Validation

F. Re-Accreditation

Correct Answer: CDEF

QUESTION 13

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. Risk rating

B. Warning signs

C. Cost of the project

D. Symptoms

Correct Answer: C

QUESTION 14

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

A. Confidentiality

B. Encryption

C. Integrity

D. Availability

Correct Answer: A

QUESTION 15

According to FIPS Publication 199, what are the three levels of potential impact on organizations in the event of a compromise on confidentiality, integrity, and availability?

A. Confidential, Secret, and High

B. Minimum, Moderate, and High

C. Low, Normal, and High

D. Low, Moderate, and High

Correct Answer: D