

QUESTIONS & ANSWERS

Kill your exam at first Attempt

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



ISA

CAP

Certified Authorization Professional

<http://killexams.com/pass4sure/exam-detail/CAP>



QUESTION: 384

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

- A. Anonymous
- B. Multi-factor
- C. Biometrics
- D. Mutual

Answer: B

QUESTION: 385

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199. What levels of potential impact are defined by FIPS 199? Each correct answer represents a complete solution. Choose all that apply.

- A. Low
- B. Moderate
- C. High
- D. Medium

Answer: A, C, D

QUESTION: 386

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

- A. Security organization
- B. Security plan
- C. Security education
- D. Information classification

Answer: B

QUESTION: 387

Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

- A. Project contractual relationship with the vendor
- B. Project communications plan
- C. Project management plan
- D. Project scope statement

Answer: C

QUESTION: 388

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

Answer: C

QUESTION: 389

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

Answer: B

QUESTION: 390

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 list containing user accounts, groups, and computers that are allowed (or denied) access to the object.
- D. It is a unique number that identifies a user, group, and computer account

Answer: C

QUESTION: 391

Which of the following is used to indicate that the software has met a defined quality level and is ready for mass distribution either by electronic means or by physical media?

- A. DAA
- B. RTM
- C. ATM
- D. CRO

Answer: B

QUESTION: 392

Which of the following processes is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

- A. Configuration management
- B. Procurement management
- C. Change management
- D. Risk management

Answer: C

QUESTION: 393

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies? Each correct answer represents a complete solution. Choose all that apply.

- A. Systematic
- B. Regulatory
- C. Advisory
- D. Informative

Answer: B, C, D

QUESTION: 394

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

Answer: A

QUESTION: 395

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.

Answer: A

For More exams visit <https://killexams.com/vendors-exam-list>



Kill your exam at First Attempt....Guaranteed!