

# ISC2

## Exam Questions CAP

ISC2 CAP Certified Authorization Professional



#### NEW QUESTION 1

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?

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

- A. Preserving high-level communications and working group relationships in an organization
- B. Facilitating the sharing of security risk-related information among authorizing officials
- C. Establishing effective continuous monitoring program for the organization
- D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

**Answer:** ACD

#### NEW QUESTION 2

Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?

- A. Information system owner
- B. Authorizing Official
- C. Chief Risk Officer (CRO)
- D. Chief Information Officer (CIO)

**Answer:** A

#### NEW QUESTION 3

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

**Answer:** CDEF

#### NEW QUESTION 4

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

- A. Mandatory Access Control
- B. Role-Based Access Control
- C. Discretionary Access Control
- D. Policy Access Control

**Answer:** B

#### NEW QUESTION 5

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

**Answer:** D

#### NEW QUESTION 6

Certification and Accreditation (C&A or CnA) is a process for implementing information security.

Which of the following is the correct order of C&A phases in a DITSCAP assessment?

- A. Definition, Validation, Verification, and Post Accreditation
- B. Verification, Definition, Validation, and Post Accreditation
- C. Verification, Validation, Definition, and Post Accreditation
- D. Definition, Verification, Validation, and Post Accreditation

**Answer:** D

#### NEW QUESTION 7

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production?

Each correct answer represents a part of the solution. Choose all that apply.

- A. NIST

- B. FIPS
- C. FISMA
- D. Office of Management and Budget (OMB)

**Answer:** CD

#### NEW QUESTION 8

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 & Configuration
- C. EC Enclave and Computing Environment
- D. Information systems acquisition, development, and maintenance

**Answer:** ABC

#### NEW QUESTION 9

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

- A. DoDD 8000.1
- B. DoD 7950.1-M
- C. DoD 5200.22-M
- D. DoD 8910.1
- E. DoD 5200.1-R

**Answer:** B

#### NEW QUESTION 10

Gary is the project manager of his organization. He is managing a project that is similar to a project his organization completed recently. Gary has decided that he will use the information from the past project to help him and the project team to identify the risks that may be present in the project. Management agrees that this checklist approach is ideal and will save time in the project.

Which of the following statement is most accurate about the limitations of the checklist analysis approach for Gary?

- A. The checklist analysis approach is fast but it is impossible to build an exhaustive checklist.
- B. The checklist analysis approach only uses qualitative analysis.
- C. The checklist analysis approach saves time, but can cost more.
- D. The checklist is also known as top down risk assessment

**Answer:** A

#### NEW QUESTION 10

What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Develop DIACAP strategy.
- B. Assign IA controls.
- C. Assemble DIACAP team.
- D. Initiate IA implementation plan.
- E. Register system with DoD Component IA Program.
- F. Conduct validation activity.

**Answer:** ABCDE

#### NEW QUESTION 14

In which type of access control do user ID and password system come under?

- A. Administrative
- B. Technical
- C. Power
- D. Physical

**Answer:** B

#### NEW QUESTION 16

You and your project team are identifying the risks that may exist within your project. Some of the risks are small risks that won't affect your project much if they happen. What should you do with these identified risk events?

- A. These risks can be accepted.
- B. These risks can be added to a low priority risk watch list.
- C. All risks must have a valid, documented risk response.
- D. These risks can be dismissed.

**Answer:** B

#### NEW QUESTION 20

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

#### NEW QUESTION 24

James work as an IT systems personnel in SoftTech Inc. He performs the following tasks: Runs regular backups and routine tests of the validity of the backup data.

Performs data restoration from the backups whenever required.

Maintains the retained records in accordance with the established information classification policy.

What is the role played by James in the organization?

- A. Manager
- B. User
- C. Owner
- D. Custodian

**Answer:** D

#### NEW QUESTION 29

A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

- A. Avoidance
- B. Mitigation
- C. Exploit
- D. Transference

**Answer:** D

#### NEW QUESTION 31

Risks with low ratings of probability and impact are included on a \_\_\_\_\_ for future monitoring.

- A. Watchlist
- B. Risk alarm
- C. Observation list
- D. Risk register

**Answer:** A

#### NEW QUESTION 32

Frank is the project manager of the NHH Project. He is working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team.

What document is Frank and the NHH Project team creating in this scenario?

- A. Project management plan
- B. Resource management plan
- C. Risk management plan
- D. Project plan

**Answer:** C

#### NEW QUESTION 36

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. Walk-through test
- C. Penetration test
- D. Paper test

**Answer:** C

#### NEW QUESTION 38

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

**Answer:** D

**NEW QUESTION 39**

In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

- A. Phase 2
- B. Phase 3
- C. Phase 1
- D. Phase 4

**Answer:** B

**NEW QUESTION 44**

A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

- A. Security law
- B. Privacy law
- C. Copyright law
- D. Trademark law

**Answer:** B

**NEW QUESTION 48**

Which of the following is a 1996 United States federal law, designed to improve the way the federal government acquires, uses, and disposes information technology?

- A. Computer Misuse Act
- B. Lanham Act
- C. Clinger-Cohen Act
- D. Paperwork Reduction Act

**Answer:** C

**NEW QUESTION 52**

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

**Answer:** B

**NEW QUESTION 55**

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. Project management plan
- B. Risk management plan
- C. Risk log
- D. Risk register

**Answer:** D

**NEW QUESTION 57**

Wendy is about to perform qualitative risk analysis on the identified risks within her project. Which one of the following will NOT help Wendy to perform this project management activity?

- A. Stakeholder register
- B. Risk register
- C. Project scope statement
- D. Risk management plan

**Answer:** A

**NEW QUESTION 58**

Which one of the following is the only output for the qualitative risk analysis process?

- A. Project management plan
- B. Risk register updates
- C. Enterprise environmental factors
- D. Organizational process assets

**Answer: B**

**NEW QUESTION 59**

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

**Answer: C**

**NEW QUESTION 61**

You and your project team are just starting the risk identification activities for a project that is scheduled to last for 18 months. Your project team has already identified a long list of risks that need to be analyzed. How often should you and the project team do risk identification?

- A. At least once per month
- B. Identify risks is an iterative process.
- C. It depends on how many risks are initially identified.
- D. Several times until the project moves into execution

**Answer: B**

**NEW QUESTION 62**

Sam is the project manager of a construction project in south Florida. This area of the United States is prone to hurricanes during certain parts of the year. As part of the project plan Sam and the project team acknowledge the possibility of hurricanes and the damage the hurricane could have on the project's deliverables, the schedule of the project, and the overall cost of the project.

Once Sam and the project stakeholders acknowledge the risk of the hurricane they go on planning the project as if the risk is not likely to happen. What type of risk response is Sam using?

- A. Mitigation
- B. Avoidance
- C. Passive acceptance
- D. Active acceptance

**Answer: C**

**NEW QUESTION 64**

Fred is the project manager of the PKL project. He is working with his project team to complete the quantitative risk analysis process as a part of risk management planning. Fred understands that once the quantitative risk analysis process is complete, the process will need to be completed again in at least two other times in the project. When will the quantitative risk analysis process need to be repeated?

- A. Quantitative risk analysis process will be completed again after the plan risk response planning and as part of procurement.
- B. Quantitative risk analysis process will be completed again after the cost management planning and as a part of monitoring and controlling.
- C. Quantitative risk analysis process will be completed again after new risks are identified and as part of monitoring and controlling.
- D. Quantitative risk analysis process will be completed again after the risk response planning and as a part of monitoring and controlling.

**Answer: D**

**NEW QUESTION 68**

You are the project manager for a construction project. The project includes a work that involves very high financial risks. You decide to insure processes so that any ill happening can be compensated. Which type of strategies have you used to deal with the risks involved with that particular work?

- A. Transfer
- B. Mitigate
- C. Accept
- D. Avoid

**Answer: A**

**NEW QUESTION 69**

Which of the following are the common roles with regard to data in an information classification program?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Custodian
- B. User
- C. Security auditor
- D. Editor
- E. Owner

**Answer: ABCE**

**NEW QUESTION 70**

Jeff, a key stakeholder in your project, wants to know how the risk exposure for the risk events is calculated during quantitative risk analysis. He is worried about the risk exposure which is too low for the events surrounding his project requirements. How is the risk exposure calculated?

- A. The probability of a risk event plus the impact of a risk event determines the true risk exposure.
- B. The risk exposure of a risk event is determined by historical information.
- C. The probability of a risk event times the impact of a risk event determines the true risk exposure.
- D. The probability and impact of a risk event are gauged based on research and in-depth analysis.

**Answer:** C

#### NEW QUESTION 71

Which of the following concepts represent the three fundamental principles of information security?  
Each correct answer represents a complete solution. Choose three.

- A. Privacy
- B. Integrity
- C. Availability
- D. Confidentiality

**Answer:** BCD

#### NEW QUESTION 73

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

- A. Chief Information Security Officer
- B. Senior Management
- C. Information Security Steering Committee
- D. Business Unit Manager

**Answer:** B

#### NEW QUESTION 77

Your organization has a project that is expected to last 20 months but the customer would really like the project completed in 18 months. You have worked on similar projects in the past and believe that you could fast track the project and reach the 18 month deadline. What increases when you fast track a project?

- A. Risks
- B. Costs
- C. Resources
- D. Communication

**Answer:** A

#### NEW QUESTION 81

The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA?

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

- A. IATO
- B. ATO
- C. IATT
- D. ATT
- E. DATO

**Answer:** ABCE

#### NEW QUESTION 82

Tom is the project manager for his organization. In his project he has recently finished the risk response planning. He tells his manager that he will now need to update the cost and schedule baselines. Why would the risk response planning cause Tom the need to update the cost and schedule baselines?

- A. New or omitted work as part of a risk response can cause changes to the cost and/or schedule baseline.
- B. Risk responses protect the time and investment of the project.
- C. Baselines should not be updated, but refined through versions.
- D. Risk responses may take time and money to implement.

**Answer:** A

#### NEW QUESTION 83

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

**Answer:** C



**NEW QUESTION 84**

You work as a project manager for BlueWell Inc. You are currently working with the project stakeholders to identify risks in your project. You understand that the qualitative risk assessment and analysis can reflect the attitude of the project team and other stakeholders to risk. Effective assessment of risk requires management of the risk attitudes of the participants. What should you, the project manager, do with assessment of identified risks in consideration of the attitude and bias of the participants towards the project risk?

- A. Document the bias for the risk events and communicate the bias with management
- B. Evaluate and document the bias towards the risk events
- C. Evaluate the bias through SWOT for true analysis of the risk events
- D. Evaluate the bias towards the risk events and correct the assessment accordingly

**Answer: D**

**NEW QUESTION 89**

Courtney is the project manager for her organization. She is working with the project team to complete the qualitative risk analysis for her project. During the analysis Courtney encourages the project team to begin the grouping of identified risks by common causes. What is the primary advantage to group risks by common causes during qualitative risk analysis?

- A. It can lead to developing effective risk responses.
- B. It can lead to the creation of risk categories unique to each project.
- C. It helps the project team realize the areas of the project most laden with risks.
- D. It saves time by collecting the related resources, such as project team members, to analyze the risk events.

**Answer: A**

**NEW QUESTION 90**

You are the program manager for your project. You are working with the project managers regarding the procurement processes for their projects. You have ruled out one particular contract type because it is considered too risky for the program. Which one of the following contract types is usually considered to be the most dangerous for the buyer?

- A. Cost plus incentive fee
- B. Time and materials
- C. Cost plus percentage of costs
- D. Fixed fee

**Answer: C**

**NEW QUESTION 91**

There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

- A. Acceptance
- B. Mitigation
- C. Sharing
- D. Transference

**Answer: A**

**NEW QUESTION 92**

What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

- A. PON
- B. ZOPA
- C. BATNA
- D. Bias

**Answer: C**

**NEW QUESTION 96**

Which of the following approaches can be used to build a security program?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Bottom-Up Approach
- B. Right-Up Approach
- C. Top-Down Approach
- D. Left-Up Approach

**Answer: AC**

**NEW QUESTION 98**

Sammy is the project manager for her organization. She would like to rate each risk based on its probability and affect on time, cost, and scope. Harry, a project team member, has never done this before and thinks Sammy is wrong to attempt this approach. Harry says that an accumulative risk score should be created, not three separate risk scores. Who is correct in this scenario?

- A. Sammy is correct, because organizations can create risk scores for each objective of the project.
- B. Harry is correct, because the risk probability and impact considers all objectives of the project.
- C. Harry is correct, the risk probability and impact matrix is the only approach to risk assessment.
- D. Sammy is correct, because she is the project manager.



**Answer:** A

**NEW QUESTION 100**

The Project Risk Management knowledge area focuses on which of the following processes?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Potential Risk Monitoring
- B. Risk Management Planning
- C. Quantitative Risk Analysis
- D. Risk Monitoring and Control

**Answer:** BCD

**NEW QUESTION 105**

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

**NEW QUESTION 109**

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

**NEW QUESTION 111**

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

**NEW QUESTION 114**

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

**NEW QUESTION 117**

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

**NEW QUESTION 122**

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**

#### NEW QUESTION 125

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**

#### NEW QUESTION 126

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**

#### NEW QUESTION 130

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**

#### NEW QUESTION 133

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**

#### NEW QUESTION 136

Amy is the project manager for her company. In her current project the organization has a very low tolerance for risk events that will affect the project schedule. Management has asked Amy to consider the affect of all the risks on the project schedule. What approach can Amy take to create a bias against risks that will affect the schedule of the project?

- A. She can have the project team pad their time estimates to alleviate delays in the project schedule.
- B. She can shift risk-laden activities that affect the project schedule from the critical path as much as possible.
- C. She can create an overall project rating scheme to reflect the bias towards risks that affect the project schedule.
- D. She can filter all risks based on their affect on schedule versus other project objectives.

**Answer: C**

#### NEW QUESTION 141

Joan is a project management consultant and she has been hired by a firm to help them identify risk events within the project. Joan would first like to examine the project documents including the plans, assumptions lists, project files, and contracts. What key thing will help Joan to discover risks within the review of the project documents?

- A. Lack of consistency between the plans and the project requirements and assumptions can be the indicators of risk in the project.
- B. The project documents will help the project manager, or Joan, to identify what risk identification approach is best to pursue.
- C. Plans that have loose definitions of terms and disconnected approaches will reveal risks.
- D. Poorly written requirements will reveal inconsistencies in the project plans and documents.

**Answer:** A

**NEW QUESTION 145**

You and your project team are just starting the risk identification activities for a project that is scheduled to last for 18 months. Your project team has already identified a long list of risks that need to be analyzed. How often should you and the project team do risk identification?

- A. At least once per month
- B. Several times until the project moves into execution
- C. It depends on how many risks are initially identified.
- D. Identify risks is an iterative process.

**Answer:** D

**NEW QUESTION 149**

Which of the following individuals informs all C&A participants about life cycle actions, security requirements, and documented user needs?

- A. IS program manager
- B. Certification Agent
- C. User representative
- D. DAA

**Answer:** A

**NEW QUESTION 150**

Gary is the project manager for his project. He and the project team have completed the qualitative risk analysis process and are about to enter the quantitative risk analysis process when Mary, the project sponsor, wants to know what quantitative risk analysis will review. Which of the following statements best defines what quantitative risk analysis will review?

- A. The quantitative risk analysis process will analyze the effect of risk events that may substantially impact the project's competing demands.
- B. The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.
- C. The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.
- D. The quantitative risk analysis seeks to determine the true cost of each identified risk event and the probability of each risk event to determine the risk exposure.

**Answer:** A

**NEW QUESTION 152**

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

**Answer:** A

**NEW QUESTION 155**

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

**Answer:** B

**NEW QUESTION 156**

Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Race conditions
- B. Social engineering
- C. Information system architectures
- D. Buffer overflows
- E. Kernel flaws
- F. Trojan horses
- G. File and directory permissions

**Answer:** ABDEFG

**NEW QUESTION 161**

Which of the following methods of authentication uses finger prints to identify users?

- A. PKI
- B. Mutual authentication
- C. Biometrics
- D. Kerberos

**Answer:** C

**NEW QUESTION 166**

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

**Answer:** A

**NEW QUESTION 169**

Which of the following phases begins with a review of the SSAA in the DITSCAP accreditation?

- A. Phase 1
- B. Phase 4
- C. Phase 3
- D. Phase 2

**Answer:** C

**NEW QUESTION 172**

Which of the following NIST documents defines impact?

- A. NIST SP 800-53
- B. NIST SP 800-26
- C. NIST SP 800-30
- D. NIST SP 800-53A

**Answer:** C

**NEW QUESTION 177**

Which of the following processes has the goal to ensure that any change does not lead to reduced or compromised security?

- A. Change control management
- B. Security management
- C. Configuration management
- D. Risk management

**Answer:** A

**NEW QUESTION 181**

In which of the following phases does the SSAA maintenance take place?

- A. Phase 3
- B. Phase 2
- C. Phase 1
- D. Phase 4

**Answer:** D

**NEW QUESTION 183**

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

**Answer:** A

**NEW QUESTION 187**

Which of the following assessment methods is used to review, inspect, and analyze assessment objects?

- A. Testing
- B. Examination
- C. Interview

D. Debugging

**Answer:** B

**NEW QUESTION 190**

Which of the following documents is used to provide a standard approach to the assessment of NIST SP 800-53 security controls?

- A. NIST SP 800-37
- B. NIST SP 800-41
- C. NIST SP 800-53A
- D. NIST SP 800-66

**Answer:** C

**NEW QUESTION 195**

What is the objective of the Security Accreditation Decision task?

- A. To determine whether the agency-level risk is acceptable or not.
- B. To make an accreditation decision
- C. To accredit the information system
- D. To approve revisions of NIACAP

**Answer:** A

**NEW QUESTION 199**

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

**Answer:** ABC

**NEW QUESTION 200**

Beth is the project manager of the BFG Project for her company. In this project Beth has decided to create a contingency response based on the performance of the project schedule. If the project schedule variance is greater than \$10,000 the contingency plan will be implemented. What is the formula for the schedule variance?

- A.  $SV = EV - PV$
- B.  $SV = EV / AC$
- C.  $SV = PV - EV$
- D.  $SV = EV / PV$

**Answer:** A

**NEW QUESTION 204**

Ned is the program manager for his organization and he's considering some new materials for his program. He and his team have never worked with these materials before and he wants to ask the vendor for some additional information, a demon, and even some samples. What type of a document should Ned send to the vendor?

- A. IFB
- B. RFI
- C. RFQ
- D. RFP

**Answer:** B

**NEW QUESTION 208**

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

**Answer:** A

**NEW QUESTION 210**

Which of the following is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls?

- A. IATT
- B. ATO
- C. IATO
- D. DATO

**Answer: C**

#### NEW QUESTION 211

Nancy is the project manager of the NHH project. She and the project team have identified a significant risk in the project during the qualitative risk analysis process. Bob is familiar with the technology that the risk is affecting and proposes to Nancy a solution to the risk event. Nancy tells Bob that she has noted his response, but the risk really needs to pass through the quantitative risk analysis process before creating responses. Bob disagrees and ensures Nancy that his response is most appropriate for the identified risk. Who is correct in this scenario?

- A. Bob is correc
- B. Bob is familiar with the technology and the risk event so his response should be implemented.
- C. Nancy is correc
- D. Because Nancy is the project manager she can determine the correct procedures for risk analysis and risk response
- E. In addition, she has noted the risk response that Bob recommends.
- F. Nancy is correc
- G. All risks of significant probability and impact should pass the quantitative risk analysis process before risk responses are created.
- H. Bob is correc
- I. Not all riskevents have to pass the quantitative risk analysis process to develop effective risk responses.

**Answer: D**

#### NEW QUESTION 216

The only output of the perform qualitative risk analysis are risk register updates. When the project manager updates the risk register he will need to include several pieces of information including all of the following except for which one?

- A. Trends in qualitative risk analysis
- B. Risk probability-impact matrix
- C. Watchlist of low-priority risks
- D. Risks grouped by categories

**Answer: B**

#### NEW QUESTION 219

You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?

- A. Risk management plan
- B. Enterprise environmental factors
- C. Staffing management plan
- D. Risk register

**Answer: A**

#### NEW QUESTION 222

The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

- A. Registration
- B. Document mission need
- C. Negotiation
- D. Initial Certification Analysis

**Answer: ABC**

#### NEW QUESTION 224

In which of the following DIACAP phases is residual risk analyzed?

- A. Phase 2
- B. Phase 4
- C. Phase 5
- D. Phase 3
- E. Phase 1

**Answer: B**

#### NEW QUESTION 226

Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

- A. They can be removed completely by taking proper actions.
- B. They can be analyzed and measured by the risk analysis process.
- C. They can be mitigated by reviewing and taking responsible actions based on possible risks.



D. They are considered an indicator of threats coupled with vulnerability.

**Answer:** BCD

**NEW QUESTION 227**

A high-profile, high-priority project within your organization is being created. Management wants you to pay special attention to the project risks and do all that you can to ensure that all of the risks are identified early in the project. Management has to ensure that this project succeeds. Management's risk aversion in this project is associated with what term?

- A. Utility function
- B. Risk conscience
- C. Quantitative risk analysis
- D. Risk mitigation

**Answer:** A

**NEW QUESTION 228**

Which of the following governance bodies directs and coordinates implementations of the information security program?

- A. Information Security Steering Committee
- B. Senior Management
- C. Business Unit Manager
- D. Chief Information Security Officer

**Answer:** D

**NEW QUESTION 230**

Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

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

**Answer:** A

**NEW QUESTION 231**

Who is responsible for the stakeholder expectations management in a high-profile, high-risk project?

- A. Project management office
- B. Project sponsor
- C. Project risk assessment officer
- D. Project manager

**Answer:** D

**NEW QUESTION 236**

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production?

Each correct answer represents a part of the solution. Choose all that apply.

- A. NIST
- B. FIPS
- C. Office of Management and Budget (OMB)
- D. FISMA

**Answer:** CD

**NEW QUESTION 241**

Which of the following refers to a process that is used for implementing information security?

- A. Certification and Accreditation (C&A)
- B. Information Assurance (IA)
- C. Five Pillars model
- D. Classic information security model

**Answer:** A

**NEW QUESTION 244**

What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?

- A. Staffing management plan
- B. Risk analysis plan
- C. Human resource management plan

D. Risk management plan

**Answer:** D

**NEW QUESTION 246**

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

**Answer:** A

**NEW QUESTION 249**

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. Project charter
- B. Risk management plan
- C. Risk register
- D. Quality management plan

**Answer:** C

**NEW QUESTION 254**

Which of the following statements about the availability concept of Information security management is true?

- A. It ensures that modifications are not made to data by unauthorized personnel or processes .
- B. It ensures reliable and timely access to resources.
- C. It determines actions and behaviors of a single individual within a system.
- D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

**Answer:** B

**NEW QUESTION 257**

Which of the following statements about System Access Control List (SACL) is true?

- A. It contains a list of any events that are set to audit for that particular object.
- B. It is a mechanism for reducing the need for globally unique IP addresses.
- C. It contains a list of both users and groups and whatever permissions they have.
- D. It exists for each and every permission entry assigned to any object.

**Answer:** A

**NEW QUESTION 261**

You are preparing to complete the quantitative risk analysis process with your project team and several subject matter experts. You gather the necessary inputs including the project's cost management plan. Why is it necessary to include the project's cost management plan in the preparation for the quantitative risk analysis process?

- A. The project's cost management plan can help you to determine what the total cost of the project is allowed to be.
- B. The project's cost management plan provides direction on how costs may be changed due to identified risks.
- C. The project's cost management plan provides control that may help determine the structure for quantitative analysis of the budget.
- D. The project's cost management plan is not an input to the quantitative risk analysis process .

**Answer:** C

**NEW QUESTION 265**

You work as a project manager for BlueWell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decided, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project which of the following are likely to increase?

- A. Quality control concerns
- B. Costs
- C. Risks
- D. Human resource needs

**Answer:** C

**NEW QUESTION 270**

Which of the following are included in Technical Controls?

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

- A. Implementing and maintaining access control mechanisms
- B. Password and resource management
- C. Configuration of the infrastructure
- D. Identification and authentication methods
- E. Conducting security-awareness training
- F. Security devices

**Answer:** ABCDF

**NEW QUESTION 275**

You are the project manager of the HJK project for your organization. You and the project team have created risk responses for many of the risk events in the project. A teaming agreement is an example of what risk response?

- A. Acceptance
- B. Mitigation
- C. Sharing
- D. Transference

**Answer:** C

**NEW QUESTION 277**

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

**Answer:** C

**NEW QUESTION 279**

Which of the following processes is described in the statement below?

"It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

- A. Perform Quantitative Risk Analysis
- B. Perform Qualitative Risk Analysis
- C. Monitor and Control Risks
- D. Identify Risks

**Answer:** C

**NEW QUESTION 280**

There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

- A. Enhance
- B. Exploit
- C. Acceptance
- D. Share

**Answer:** C

**NEW QUESTION 283**

Adrian is a project manager for a new project using a technology that has recently been released and there's relatively little information about the technology. Initial testing of the technology makes the use of it look promising, but there's still uncertainty as to the longevity and reliability of the technology. Adrian wants to consider the technology factors a risk for her project. Where should she document the risks associated with this technology so she can track the risk status and responses?

- A. Project charter
- B. Risk register
- C. Project scope statement
- D. Risk low-level watch list

**Answer:** B

**NEW QUESTION 285**

Gary is the project manager for his organization. He is working with the project stakeholders on the project requirements and how risks may affect their project. One of the stakeholders is confused about what constitutes risks in the project. Which of the following is the most accurate definition of a project risk?

- A. It is an uncertain event that can affect the project costs.
- B. It is an uncertain event or condition within the project execution.
- C. It is an uncertain event that can affect at least one project objective.
- D. It is an unknown event that can affect the project scope.

**Answer:** C

#### NEW QUESTION 290

Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives?

- A. NIST SP 800-53A
- B. NIST SP 800-26
- C. NIST SP 800-53
- D. NIST SP 800-59
- E. NIST SP 800-60
- F. NIST SP 800-37

**Answer:** B

#### NEW QUESTION 291

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. Business continuity plan
- B. Continuity of Operations Plan
- C. Disaster recovery plan
- D. Contingency plan

**Answer:** D

#### NEW QUESTION 296

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. Informative
- C. Regulatory
- D. Advisory

**Answer:** BCD

#### NEW QUESTION 300

Harry is a project manager of a software development project. In the early stages of planning, he and the stakeholders operated with the belief that the software they were developing would work with their organization's current computer operating system. Now that the project team has started developing the software it has become apparent that the software will not work with nearly half of the organization's computer operating systems. The incorrect belief Harry had in the software compatibility is an example of what in project management?

- A. Issue
- B. Risk
- C. Constraint
- D. Assumption

**Answer:** D

#### NEW QUESTION 301

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.

**Answer:** D

#### NEW QUESTION 306

Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

- A. It depends on what the outcome of a lawsuit will determine.
- B. No, the ZAS Corporation did not complete all of the work.
- C. It depends on what the termination clause of the contract stipulates.
- D. Yes, the ZAS Corporation did not choose to terminate the contract work.

**Answer:** C

#### NEW QUESTION 309

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 U.S. Federal Government information security standards?

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

- A. SA System and Services Acquisition

- B. CA Certification, Accreditation, and Security Assessments
- C. IR Incident Response
- D. Information systems acquisition, development, and maintenance

**Answer:** ABC

**NEW QUESTION 311**

Jenny is the project manager for the NBT projects. She is working with the project team and several subject matter experts to perform the quantitative risk analysis process. During this process she and the project team uncover several risks events that were not previously identified. What should Jenny do with these risk events?

- A. The events should be determined if they need to be accepted or responded to.
- B. The events should be entered into qualitative risk analysis.
- C. The events should continue on with quantitative risk analysis.
- D. The events should be entered into the risk register.

**Answer:** D

**NEW QUESTION 314**

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

- A. Authenticity
- B. Confidentiality
- C. Availability
- D. Integrity

**Answer:** B

**NEW QUESTION 315**

Harry is the project manager of the MMQ Construction Project. In this project Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States. Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project's deadline. Management asked Harry to find a supplier who will guarantee the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?

- A. Acceptance
- B. Mitigation
- C. Avoidance
- D. Transference

**Answer:** B

**NEW QUESTION 317**

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 countermeasures
- B. Identifying the risk
- C. Assessing the impact of potential threats
- D. Identifying the accused

**Answer:** ABC

**NEW QUESTION 320**

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.

**Answer:** D

**NEW QUESTION 325**

Diane is the project manager of the HGF Project. A risk that has been identified and analyzed in the project planning processes is now coming into fruition. What individual should respond to the risk with the preplanned risk response?

- A. Diane
- B. Risk owner
- C. Subject matter expert
- D. Project sponsor

**Answer:** B

**NEW QUESTION 327**

Which of the following acts promote a risk-based policy for cost effective security?  
Each correct answer represents a part of the solution. Choose all that apply.

- A. Clinger-Cohen Act
- B. Lanham Act
- C. Computer Misuse Act
- D. Paperwork Reduction Act (PRA)

**Answer:** AD

**NEW QUESTION 332**

To help review or design security controls, they can be classified by several criteria. One of these criteria is based on time. According to this criteria, which of the following controls are intended to prevent an incident from occurring?

- A. Adaptive controls
- B. Preventive controls
- C. Detective controls
- D. Corrective controls

**Answer:** B

**NEW QUESTION 337**

You are the project manager for a construction project. The project involves casting of a column in a very narrow space. Because of lack of space, casting it is highly dangerous. High technical skill will be required for casting that column. You decide to hire a local expert team for casting that column. Which of the following types of risk response are you following?

- A. Mitigation
- B. Avoidance
- C. Transference
- D. Acceptance

**Answer:** C

**NEW QUESTION 340**

Which of the following statements about the authentication concept of information security management is true?

- A. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual.
- B. It ensures that modifications are not made to data by unauthorized personnel or processes .
- C. It establishes the users' identity and ensures that the users are who they say they are.
- D. It ensures the reliable and timely access to resources.

**Answer:** C

**NEW QUESTION 343**

Which of the following groups represents the most likely source of an asset loss through the inappropriate use of computers?

- A. Hackers
- B. Visitors
- C. Customers
- D. Employees

**Answer:** D

**NEW QUESTION 347**

Certification and Accreditation (C&A or CnA) is a process for implementing information security.  
Which of the following is the correct order of C&A phases in a DITSCAP assessment?

- A. Definition, Validation, Verification, and Post Accreditation
- B. Verification, Definition, Validation, and Post Accreditation
- C. Definition, Verification, Validation, and Post Accreditation
- D. Verification, Validation, Definition, and Post Accreditation

**Answer:** C

**NEW QUESTION 348**

You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

- A. Qualitative risk analysis
- B. Quantitative analysis
- C. Historical information
- D. Rolling wave planning

**Answer:** A



**NEW QUESTION 351**

Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

- A. The custodian implements the information classification scheme after the initial assignment by the operations manager.
- B. The datacustodian implements the information classification scheme after the initial assignment by the data owner.
- C. The data owner implements the information classification scheme after the initial assignment by the custodian.
- D. The custodian makes the initialinformation classification assignments, and the operations manager implements the scheme.

**Answer: B**

**NEW QUESTION 355**

In which of the following Risk Management Framework (RMF) phases is a risk profile created for threats?

- A. Phase 3
- B. Phase 1
- C. Phase 2
- D. Phase 0

**Answer: C**

**NEW QUESTION 359**

In which of the following DITSCAP phases is the SSAA developed?

- A. Phase 4
- B. Phase 2
- C. Phase 1
- D. Phase 3

**Answer: C**

**NEW QUESTION 361**

Which of the following recovery plans includes a monitoring process and triggers for initiating planned actions?

- A. Contingency plan
- B. Business continuity plan
- C. Disaster recovery plan
- D. Continuity of Operations Plan

**Answer: A**

**NEW QUESTION 362**

Which of the following NIST documents includes components for penetration testing?

- A. NIST SP 800-53
- B. NIST SP 800-26
- C. NIST SP 800-37
- D. NIST SP 800-30

**Answer: D**

**NEW QUESTION 366**

Which of the following processes has the goal to ensure that any change does not lead to reduced or compromised security?

- A. Risk management
- B. Security management
- C. Configuration management
- D. Changecontrol management

**Answer: D**

**NEW QUESTION 367**

Which of the following is not a part of Identify Risks process?

- A. Decision tree diagram
- B. Cause and effect diagram
- C. Influence diagram
- D. System or process flow chart

**Answer: A**

**NEW QUESTION 370**

In which of the following phases does the SSAA maintenance take place?

- A. Phase 4

- B. Phase 2
- C. Phase 1
- D. Phase 3

**Answer:** A

**NEW QUESTION 372**

Which of the following statements is true about the continuous monitoring process?

- A. It takes place in the middle of system security accreditation.
- B. It takes place before and after system security accreditation.
- C. It takes place before the initial system security accreditation.
- D. It takes place after the initial system security accreditation.

**Answer:** D

**NEW QUESTION 376**

In which of the following phases does the change management process start?

- A. Phase 2
- B. Phase 1
- C. Phase 4
- D. Phase 3

**Answer:** C

**NEW QUESTION 381**

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

- A. Interview
- B. Deviation
- C. Examination
- D. Testing

**Answer:** D

**NEW QUESTION 383**

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

**Answer:** B

**NEW QUESTION 388**

In which of the following elements of security does the object retain its veracity and is intentionally modified by the authorized subjects?

- A. Integrity
- B. Nonrepudiation
- C. Availability
- D. Confidentiality

**Answer:** A

**NEW QUESTION 393**

Which of the following relations correctly describes total risk?

- A. Total Risk = Threats x Vulnerability x Asset Value
- B. Total Risk = Viruses x Vulnerability x Asset Value
- C. Total Risk = Threats x Exploit x Asset Value
- D. Total Risk = Viruses x Exploit x Asset Value

**Answer:** A

**NEW QUESTION 398**

Which of the following individuals is responsible for the final accreditation decision?

- A. Certification Agent
- B. User Representative
- C. Information System Owner
- D. Risk Executive

**Answer:** C

**NEW QUESTION 399**

A \_\_\_\_\_ points to a statement in a policy or procedure that helps determine a course of action.

- A. Comment
- B. Guideline
- C. Procedure
- D. Baseline

**Answer: B**

**NEW QUESTION 402**

Which of the following are the types of assessment tests addressed in NIST SP 800-53A?

- A. Functional, penetration, validation
- B. Validation, evaluation, penetration
- C. Validation, penetration, evaluation
- D. Functional, structural, penetration

**Answer: D**

**NEW QUESTION 404**

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

- A. Commoncontrol provider
- B. Information system owner
- C. Authorizing official
- D. Chief information officer

**Answer: B**

**NEW QUESTION 409**

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

- A. DoD 5200.22-M
- B. DoD 5200.1-R
- C. DoD 8910.1
- D. DoDD 8000.1
- E. DoD 7950.1-M

**Answer: E**

**NEW QUESTION 411**

Management wants you to create a visual diagram of what resources will be utilized in the project deliverables. What type of a chart is management asking you to create?

- A. Work breakdown structure
- B. Roles and responsibility matrix
- C. Resource breakdown structure
- D. RACI chart

**Answer: C**

**NEW QUESTION 412**

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

- A. Authenticity
- B. Integrity
- C. Availability
- D. Confidentiality

**Answer: D**

**NEW QUESTION 413**

Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

- A. No, the ZAS Corporation did not complete all of the work.
- B. Yes, the ZAS Corporation did not choose to terminate the contract work.
- C. It depends on what the outcome of a lawsuit will determine.
- D. It depends on what the terminationclause of the contract stipulates

**Answer: D**

#### NEW QUESTION 414

There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

- A. Enhance
- B. Exploit
- C. Acceptance
- D. Share

**Answer: C**

#### NEW QUESTION 415

The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE?

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

- A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
- B. An ISSO takes part in the development activities that are required to implement system changes.
- C. An ISSE provides advice on the continuous monitoring of the information system.
- D. An ISSE provides advice on the impacts of system changes.
- E. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).

**Answer: CDE**

#### NEW QUESTION 419

Which one of the following is the only output for the qualitative risk analysis process?

- A. Enterprise environmental factors
- B. Project management plan
- C. Risk register updates
- D. Organizational process assets

**Answer: C**

#### NEW QUESTION 420

Which of the following RMF phases is known as risk analysis?

- A. Phase 0
- B. Phase 1
- C. Phase 2
- D. Phase 3

**Answer: C**

#### NEW QUESTION 423

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**

#### NEW QUESTION 424

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**

#### NEW QUESTION 427

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: BCD**

**NEW QUESTION 429**

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

**NEW QUESTION 432**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### CAP Practice Exam Features:

- \* CAP Questions and Answers Updated Frequently
- \* CAP Practice Questions Verified by Expert Senior Certified Staff
- \* CAP Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* CAP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CAP Practice Test Here](#)**