

# ISC2

## Exam Questions CAP

ISC2 CAP Certified Authorization Professional



#### NEW QUESTION 1

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

- A. FITSAF
- B. FIPS 102
- C. OCTAVE
- D. DITSCAP

**Answer:** B

#### NEW QUESTION 2

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 3

System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan?  
Each correct answer represents a part of the solution. Choose all that apply.

- A. Post-Authorization
- B. Pre-certification
- C. Post-certification
- D. Certification
- E. Authorization

**Answer:** ABDE

#### NEW QUESTION 4

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Secure accreditation
- B. Type accreditation
- C. System accreditation
- D. Site accreditation

**Answer:** BCD

#### NEW QUESTION 5

There are five inputs to the quantitative risk analysis process. Which one of the following is NOT an input to the perform quantitative risk analysis process?

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

**Answer:** D

#### NEW QUESTION 6

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. Risk response plan
- B. Quantitative analysis
- C. Risk response
- D. Contingency reserve

**Answer:** D

#### NEW QUESTION 7

The phase 3 of the Risk Management Framework (RMF) process is known as mitigation planning.  
Which of the following processes take place in phase 3?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Identify threats, vulnerabilities, and controls that will be evaluated.
- B. Document and implement a mitigation plan.
- C. Agree on a strategy to mitigate risks.
- D. Evaluate mitigation progress and plan next assessment.

**Answer:** BCD

#### NEW QUESTION 8

Adrian is the project manager of the NHP Project. In her project there are several work packages that deal with electrical wiring. Rather than to manage the risk internally she has decided to hire a vendor to complete all work packages that deal with the electrical wiring. By removing the risk internally to a licensed electrician Adrian feels more comfortable with project team being safe. What type of risk response has Adrian used in this example?

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

**Answer:** B

#### NEW QUESTION 9

Which of the following refers to the ability to ensure that the data is not modified or tampered with?

- A. Confidentiality
- B. Availability
- C. Integrity
- D. Non-repudiation

**Answer:** C

#### NEW QUESTION 10

System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.

- A. Pre-certification
- B. Certification
- C. Post-certification
- D. Authorization
- E. Post-Authorization

**Answer:** ABDE

#### NEW QUESTION 10

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 15

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 19

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

**Answer:** ABCDEG

**NEW QUESTION 23**

You are the project manager of the NHH project for your company. You have completed the first round of risk management planning and have created four outputs of the risk response planning process. Which one of the following is NOT an output of the risk response planning?

- A. Risk-related contract decisions
- B. Project document updates
- C. Risk register updates
- D. Organizational process assets updates

**Answer:** D

**NEW QUESTION 28**

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

- A. OCTAVE
- B. FITSAF
- C. DITSCAP
- D. FIPS 102

**Answer:** D

**NEW QUESTION 32**

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 37**

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 40**

Jenny is the project manager of the NHJ Project for her company. She has identified several positive risk events within the project and she thinks these events can save the project time and money. You, a new team member wants to know that how many risk responses are available for a positive risk event. What will Jenny reply to you?

- A. Four
- B. Seven
- C. Acceptance is the only risk response for positive risk events.
- D. Three

**Answer:** A

**NEW QUESTION 42**

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 45**

Which of the following NIST Special Publication documents provides a guideline on network security testing?

- A. NIST SP 800-60
- B. NIST SP 800-53A
- C. NIST SP 800-37
- D. NIST SP 800-42
- E. NIST SP 800-59

F. NIST SP 800-53

**Answer:** D

**NEW QUESTION 46**

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 51**

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

**Answer:** D

**NEW QUESTION 54**

You work as a project manager for SoftTech Inc. You are working with the project stakeholders to begin the qualitative risk analysis process. You will need all of the following as inputs to the qualitative risk analysis process except for which one?

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

**Answer:** C

**NEW QUESTION 58**

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 62**

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 67**

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 72**

Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

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

**Answer:** D

#### NEW QUESTION 75

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy?

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

- A. Who is expected to exploit the vulnerability?
- B. What is being secured?
- C. Where is the vulnerability, threat, or risk?
- D. Who is expected to comply with the policy?

**Answer:** BCD

#### NEW QUESTION 77

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 78

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

#### NEW QUESTION 82

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

#### NEW QUESTION 83

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 88

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

#### NEW QUESTION 92

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 97

John is the project manager of the NHQ Project for his company. His project has 75 stakeholders, some of which are external to the organization. John needs to make certain that he communicates about risk in the most appropriate method for the external stakeholders. Which project management plan will be the best guide for John to communicate to the external stakeholders?

- A. Communications Management Plan
- B. Risk Management Plan
- C. Project Management Plan
- D. Risk Response Plan

**Answer:** A

#### NEW QUESTION 100

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 103

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 107

Which of the following formulas was developed by FIPS 199 for categorization of an information type?

- A. SC information type = {(confidentiality, controls), (integrity, controls), (authentication, controls)}
- B. SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}
- C. SC information type = {(confidentiality, risk), (integrity, risk), (availability, risk)}
- D. SC information type = {(Authentication, impact), (integrity, impact), (availability, impact)}

**Answer:** B

#### NEW QUESTION 112

Which of the following formulas was developed by FIPS 199 for categorization of an information system?

- A. SC information system = {(confidentiality, impact), (integrity, controls), (availability, risk)}
- B. SC information system = {(confidentiality, impact), (integrity, impact), (availability, impact)}
- C. SC information system = {(confidentiality, controls), (integrity, controls), (availability, controls)}
- D. SC information system = {(confidentiality, risk), (integrity, impact), (availability, controls)}

**Answer:** B

#### NEW QUESTION 113

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. Where should you document the proposed responses and the current status of all identified risks?

- A. Risk management plan
- B. Stakeholder management strategy
- C. Risk register
- D. Lessons learned documentation

**Answer:** C



**NEW QUESTION 116**

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

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

**Answer: B**

**NEW QUESTION 119**

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 NGB Company to fulfill the order. The NGB 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 121**

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 correct
- B. Bob is familiar with the technology and the risk event so his response should be implemented.
- C. Nancy is correct
- 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 correct
- G. All risks of significant probability and impact should pass the quantitative risk analysis process before risk responses are created.
- H. Bob is correct
- I. Not all risk events have to pass the quantitative risk analysis process to develop effective risk responses.

**Answer: D**

**NEW QUESTION 122**

Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?

- A. At every status meeting the project team project risk management is an agenda item.
- B. Project risk management happens at every milestone.
- C. Project risk management has been concluded with the project planning.
- D. Project risk management is scheduled for every month in the 18-month project.

**Answer: A**

**NEW QUESTION 127**

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 128**

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 133**

Which of the following roles is used to ensure that the confidentiality, integrity, and availability of the services are maintained to the levels approved on the Service Level Agreement (SLA)?



- A. The Change Manager
- B. The IT Security Manager
- C. The Service Level Manager
- D. The Configuration Manager

**Answer:** B

#### NEW QUESTION 137

You are the project manager of the GHY Project for your company. You have completed the risk response planning with your project team. You now need to update the WBS. Why would the project manager need to update the WBS after the risk response planning process? Choose the best answer.

- A. Because of risks associated with work packages
- B. Because of work that was omitted during the WBS creation
- C. Because of risk responses that are now activities
- D. Because of new work generated by the risk responses

**Answer:** D

#### NEW QUESTION 141

The risk transference is referred to the transfer of risks to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Which one of the following is NOT an example of the transference risk response?

- A. Use of insurance
- B. Life cycle costing
- C. Warranties
- D. Performance bonds

**Answer:** B

#### NEW QUESTION 143

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 146

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 151

Tracy is the project manager of the NLT Project for her company. The NLT Project is scheduled to last 14 months and has a budget at completion of \$4,555,000. Tracy's organization will receive a bonus of \$80,000 per day that the project is completed early up to \$800,000. Tracy realizes that there are several opportunities within the project to save on time by crashing the project work. Crashing the project is what type of risk response?

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

**Answer:** C

#### NEW QUESTION 153

Lisa is the project manager of the SQL project for her company. She has completed the risk response planning with her project team and is now ready to update the risk register to reflect the risk response. Which of the following statements best describes the level of detail Lisa should include with the risk responses she has created?

- A. The level of detail is set by historical information.
- B. The level of detail must define exactly the risk response for each identified risk.
- C. The level of detail is set of project risk governance.
- D. The level of detail should correspond with the priority ranking

**Answer:** D

#### NEW QUESTION 157

The Identify Risk process determines the risks that affect the project and document their characteristics. Why should the project team members be involved in the Identify Risk process?

- A. They are the individuals that will have the best responses for identified risks events within the project.
- B. They are the individuals that are most affected by the risk events.
- C. They are the individuals that will need a sense of ownership and responsibility for the risk events.
- D. They are the individuals that will most likely cause and respond to the risk events.

**Answer:** C

#### NEW QUESTION 160

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

**Answer:** D

#### NEW QUESTION 164

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 5
- C. Level 4
- D. Level 1
- E. Level 3

**Answer:** E

#### NEW QUESTION 166

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

#### NEW QUESTION 171

Which of the following individuals makes the final accreditation decision?

- A. ISSE
- B. DAA
- C. CRO
- D. ISSO

**Answer:** B

#### NEW QUESTION 173

Virginia is the project manager for her organization. She has hired a subject matter expert to interview the project stakeholders on certain identified risks within the project. The subject matter expert will assess the risk event with what specific goal in mind?

- A. To determine the bias of the risk event based on each person interviewed
- B. To determine the probability and cost of the risk event
- C. To determine the validity of each risk event
- D. To determine the level of probability and impact for each risk event

**Answer:** D

#### NEW QUESTION 175

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 180**

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 183**

In what portion of a project are risk and opportunities greatest and require intense planning and anticipation of risk events?

- A. Planning
- B. Executing
- C. Closing
- D. Initiating

**Answer:** D

**NEW QUESTION 186**

You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

- A. It is a risk that remains because no risk response is taken.
- B. It is a risk that remains after planned risk responses are taken.
- C. It is a risk that can not be addressed by a risk response.
- D. It is a risk that will remain no matter what type of risk response is offered.

**Answer:** B

**NEW QUESTION 189**

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 194**

Ned is the project manager of the HNN project for your company. Ned has asked you to help him complete some probability distributions for his project. What portion of the project will you most likely use for probability distributions?

- A. Uncertainty in values such as duration of schedule activities
- B. Bias towards risk in new resources
- C. Risk probability and impact matrixes
- D. Risk identification

**Answer:** A

**NEW QUESTION 199**

What are the responsibilities of a system owner?

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

- A. Integrates security considerations into application and system purchasing decisions and development projects.
- B. Ensures that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.
- C. Ensures that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on.
- D. Ensures that the necessary security controls are in place.

**Answer:** ABC

**NEW QUESTION 201**

Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

- A. DITSCAP

- B. NIACAP
- C. NSA-IAM
- D. ASSET

**Answer:** B

**NEW QUESTION 205**

Which of the following system security policies is used to address specific issues of concern to the organization?

- A. Program policy
- B. Issue-specific policy
- C. Informative policy
- D. System-specific policy

**Answer:** B

**NEW QUESTION 209**

What does RTM stand for?

- A. Resource Testing Method
- B. Replaced Traceability Matrix
- C. Requirements Traceability Matrix
- D. Resource Tracking Matrix

**Answer:** C

**NEW QUESTION 213**

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 215**

Which of the following is a risk that is created by the response to another risk?

- A. Secondary risk
- B. Residual risk
- C. Positive risk
- D. Negative risk

**Answer:** A

**NEW QUESTION 216**

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 217**

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 222**

Which of the following C&A professionals plays the role of an advisor?

- A. Information System Security Engineer (ISSE)
- B. Chief Information Officer (CIO)
- C. Authorizing Official
- D. Information Owner

**Answer:** A

**NEW QUESTION 223**

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

**Answer:** A

**NEW QUESTION 228**

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. Risk responses may take time and money to implement.
- D. Baselines should not be updated, but refined through versions.

**Answer:** A

**NEW QUESTION 231**

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

**Answer:** B

**NEW QUESTION 236**

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

**NEW QUESTION 240**

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

**NEW QUESTION 245**

.....

## 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](#)**