

# ISC2

## Exam Questions CAP

ISC2 CAP Certified Authorization Professional



#### NEW QUESTION 1

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

**Answer:** ACE

#### 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

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 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

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

**Answer:** AD

#### NEW QUESTION 6

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 7

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. Validation
- B. Re-Accreditation

- C. Verification
- D. System Definition
- E. Identification
- F. Accreditation

**Answer:** ABCD

#### NEW QUESTION 8

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 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

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 10

Neil works as a project manager for SoftTech Inc. He is working with Tom, the COO of his company, on several risks within the project. Tom understands that through qualitative analysis Neil has identified many risks in the project. Tom's concern, however, is that the priority list of these risk events are sorted in "high-risk," "moderate-risk," and "low-risk" as conditions apply within the project. Tom wants to know that is there any other objective on which Neil can make the priority list for project risks. What will be Neil's reply to Tom?

- A. Risk may be listed by the responses in the near-term
- B. Risks may be listed by categories
- C. Risks may be listed by the additional analysis and response
- D. Risks may be listed by priority separately for schedule, cost, and performance

**Answer:** D

#### NEW QUESTION 13

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 14

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 15

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 19

Which of the following roles is also known as the accreditor?

- A. Chief Risk Officer
- B. Data owner
- C. Designated Approving Authority
- D. Chief Information Officer

**Answer:** C

#### NEW QUESTION 20

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 24

You are the project manager of the NNH Project. In this project you have created a contingency response that the schedule performance index should be less than 0.93. The NHH Project has a budget at completion of \$945,000 and is 45 percent complete though the project should be 49 percent complete. The project has spent \$455,897 to reach the 45 percent complete milestone.

What is the project's schedule performance index?

- A. 1.06
- B. 0.92
- C. -\$37,800
- D. 0.93

**Answer:** B

#### NEW QUESTION 29

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-CohenAct
- D. Paperwork Reduction Act

**Answer:** C

#### NEW QUESTION 34

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

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

**Answer:** A

#### NEW QUESTION 35

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 39**

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 41**

Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

- A. The Supplier Manager
- B. The IT Service Continuity Manager
- C. The Service Catalogue Manager
- D. The Configuration Manager

**Answer:** A

**NEW QUESTION 45**

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 46**

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

**Answer:** ABCD

**NEW QUESTION 48**

You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

- A. Sharing
- B. Avoidance
- C. Transference
- D. Exploiting

**Answer:** C

**NEW QUESTION 49**

You are the project manager of the GHQ project for your company. You are working you're your project team to prepare for the qualitative risk analysis process. Mary, a project team member, does not understand why you need to complete qualitative risks analysis. You explain to Mary that qualitative risks analysis helps you determine which risks need additional analysis. There are also some other benefits that qualitative risks analysis can do for the project. Which one of the following is NOT an accomplishment of the qualitative risk analysis process?

- A. Cost of the risk impact if the risk event occurs
- B. Corresponding impact on project objectives
- C. Time frame for a risk response
- D. Prioritization of identified risk events based on probability and impact

**Answer:** A

**NEW QUESTION 54**

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 55**

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 56**

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 57**

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 59**

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 62**

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 63**

Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

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

**Answer:** B

**NEW QUESTION 67**

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 68

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 69

You are the project manager of the GHY project for your organization. You are working with your project team to begin identifying risks for the project. As part of your preparation for identifying the risks within the project you will need eleven inputs for the process. Which one of the following is NOT an input to the risk identification process?

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

**Answer:** C

#### NEW QUESTION 70

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 74

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 77

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 81

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

- A. Teaming agreements
- B. Crashing the project
- C. Transference
- D. Fast tracking the project



**Answer:** B

**NEW QUESTION 86**

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 90**

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 92**

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 ResponsePlan

**Answer:** A

**NEW QUESTION 95**

You are the project manager of the NNH Project. In this project you have created a contingency response that the schedule performance index should be less than 0.93. The NHH Project has a budget at completion of \$945,000 and is 45 percent complete though the project should be 49 percent complete. The project has spent \$455,897 to reach the 45 percent complete milestone. What is the project's schedule performance index?

- A. 1.06
- B. 0.93
- C. -\$37,800
- D. 0.92

**Answer:** D

**NEW QUESTION 98**

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 101**

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 106**

What approach can a project manager use to improve the project's performance during qualitative risk analysis?

- A. Create a risk breakdown structure and delegate the risk analysis to the appropriate project team members.
- B. Focus on high-priority risks.



- C. Focus on near-term risks first.
- D. Analyze as many risks as possible regardless of who initiated the risk event.

**Answer:** B

#### NEW QUESTION 108

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 110

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 111

Rob is the project manager of the IDLK Project for his company. This project has a budget of \$5,600,000 and is expected to last 18 months. Rob has learned that a new law may affect how the project is allowed to proceed - even though the organization has already invested over \$750,000 in the project. What risk response is the most appropriate for this instance?

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

**Answer:** D

#### NEW QUESTION 112

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 114

You are the project manager of the GGH Project in your company. Your company is structured as a functional organization and you report to the functional manager that you are ready to move onto the quantitative risk analysis process. What things will you need as inputs for the quantitative risk analysis of the project in this scenario?

- A. You will need the risk register, risk management plan, permission from the functional manager, and any relevant organizational process assets.
- B. You will need the risk register, risk management plan, outputs of qualitative risk analysis, and any relevant organizational process assets.
- C. You will need the risk register, risk management plan, cost management plan, schedule management plan, and any relevant organizational process assets.
- D. Quantitative risk analysis does not happen through the project manager in a functional structure.

**Answer:** C

#### NEW QUESTION 116

Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process?

- A. Senior Agency Information Security Officer
- B. Authorizing Official
- C. Chief Information Officer
- D. Common Control Provider

**Answer:** D

**NEW QUESTION 119**

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

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

**Answer:** A

**NEW QUESTION 120**

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 are tested and reviewed?

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

**Answer:** C

**NEW QUESTION 121**

Information Security management is a process of defining the security controls in order to protect information assets. The first action of a management program to implement information security is to have a security program in place. What are the objectives of a security program?  
Each correct answer represents a complete solution. Choose all that apply.

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

**Answer:** ACD

**NEW QUESTION 123**

You are the project manager of the NNQ Project for your company and are working you??re your project team to define contingency plans for the risks within your project. Mary, one of your project team members, asks what a contingency plan is. Which of the following statements best defines what a contingency response is?

- A. Some responses are designed for use only if certain events occur.
- B. Some responses have a cost and a time factor to consider for each risk event.
- C. Some responses must counteract pending risk events.
- D. Quantified risks should always have contingency responses.

**Answer:** A

**NEW QUESTION 128**

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 132**

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 133**

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 135

The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented?

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

- A. Configuration status accounting
- B. Configuration change control
- C. Configuration deployment
- D. Configuration audits
- E. Configuration identification
- F. Configuration implementation

**Answer:** ABDE

#### NEW QUESTION 137

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 138

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 139

BS 7799 is an internationally recognized ISM standard that provides high level, conceptual recommendations on enterprise security. BS 7799 is basically divided into three parts. Which of the following statements are true about BS 7799?

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

- A. BS 7799 Part 1 was adopted by ISO as ISO/IEC 27001 in November 2005.
- B. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.
- C. BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards Institute (BSI) in 1995.
- D. BS 7799 Part 3 was published in 2005, covering risk analysis and management.

**Answer:** BCD

#### NEW QUESTION 141

Diana is the project manager of the QPS project for her company. In this project Diana and the project team have identified a pure risk. Diana and the project team decided, along with the key stakeholders, to remove the pure risk from the project by changing the project plan altogether.

What is a pure risk?

- A. It is a risk event that only has a negative side, such as loss of life or limb.
- B. It is a risk event that cannot be avoided because of the order of the work.
- C. It is a risk event that is created by a risk response.
- D. It is a risk event that is generated due to errors or omission in the project work.

**Answer:** A

#### NEW QUESTION 145

You work as a project manager for BlueWell Inc. You are about to complete the quantitative risk analysis process for your project. You can use three available tools and techniques to complete this process. Which one of the following is NOT a tool or technique that is appropriate for the quantitative risk analysis process?

- A. Quantitative risk analysis and modeling techniques
- B. Data gathering and representation techniques
- C. Expert judgment
- D. Organizational process assets

**Answer:** D

#### NEW QUESTION 147

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 148

Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Protect society, the commonwealth, and the infrastructure.
- B. Act honorably, honestly, justly, responsibly, and legally.
- C. Provide diligent and competent service to principals.
- D. Give guidance for resolving good versus good and bad versus baddilemmas.

**Answer:** ABC

#### NEW QUESTION 152

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

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

**Answer:** ABC

#### NEW QUESTION 154

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

**Answer:** ABC

#### NEW QUESTION 155

Mark works as a project manager for TechSoft Inc. Mark, the project team, and the key project stakeholders have completed a round of qualitative risk analysis. He needs to update the risk register with his findings so that he can communicate the risk results to the project stakeholders - including management. Mark will need to update all of the following information except for which one?

- A. Watchlist of low-priority risks
- B. Prioritized list of quantified risks
- C. Risks grouped by categories
- D. Trends in qualitative risk analysis

**Answer:** B

#### NEW QUESTION 160

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 163

Henry is the project manager of the QBG Project for his company. This project has a budget of \$4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work.  
What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?

- A. Cost change control system
- B. Scope change control system
- C. Integrated change control
- D. Configuration management system

**Answer:** D

**NEW QUESTION 165**

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

- A. To implement the design of system architecture
- B. To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
- C. To assess the degree of consistency between the system documentation and its implementation
- D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

**Answer:** BCD

**NEW QUESTION 167**

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 170**

You are the project manager of the NHQ project for your company. Management has told you that you must implement an agreed upon contingency response if the Cost Performance Index in your project is less than 0.90. Consider that your project has a budget at completion of \$250,000 and is 60 percent complete. You are scheduled to be however, 75 percent complete, and you have spent \$165,000 to date. What is the Cost Performance Index for this project to determine if the contingency response should happen?

- A. 0.88
- B. 0.80
- C. -\$37,500
- D. 0.91

**Answer:** D

**NEW QUESTION 175**

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 178**

Fred is the project manager of the CPS project. He is working with his project team to prioritize the identified risks within the CPS project. He and the team are prioritizing risks for further analysis or action by assessing and combining the risks probability of occurrence and impact. What process is Fred completing?

- A. Risk identification
- B. Perform qualitative analysis
- C. Perform quantitative analysis
- D. Risk Breakdown Structure creation

**Answer:** B

**NEW QUESTION 182**

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 186**



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 191**

You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?

- A. Risk identification
- B. Qualitative risk analysis
- C. Risk response implementation
- D. Quantitative risk analysis

**Answer:** D

**NEW QUESTION 193**

Which of the following persons is responsible for testing and verifying whether the security policy is properly implemented, and the derived security solutions are adequate or not?

- A. Auditor
- B. User
- C. Data custodian
- D. Data owner

**Answer:** A

**NEW QUESTION 197**

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 202**

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 205**

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 207**

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 211**

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 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 218**

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 223**

For which of the following reporting requirements are continuous monitoring documentation reports used?

- A. FISMA
- B. NIST
- C. HIPAA
- D. FBI

**Answer:** A

**NEW QUESTION 224**

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 229**

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

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

**Answer:** B

**NEW QUESTION 230**

Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

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

**Answer:** A

**NEW QUESTION 234**

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 239**

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

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

**Answer:** C

**NEW QUESTION 244**

.....

## 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](#)**