

ISC2

Exam Questions CAP

ISC2 CAP Certified Authorization Professional



NEW QUESTION 1

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 2

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 3

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 4

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 5

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 6

Which of the following is a subset discipline of Corporate Governance focused on information security systems and their performance and risk management?

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

Answer: B

NEW QUESTION 7

Ben is the project manager of the YHT Project for his company. Alice, one of his team members, is confused about when project risks will happen in the project. Which one of the following statements is the most accurate about when project risk happens?

- A. Project risk can happen at any moment.
- B. Project risk is uncertain, so no one can predict when the event will happen.
- C. Project risk happens throughout the project execution.
- D. Project risks always in the future.

Answer: D

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

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 10

Which of the following is an entry in an object's discretionary access control list (DACL) that grants permissions to a user or group?

- A. Access control entry (ACE)
- B. Discretionary access control entry (DACE)
- C. Access control list (ACL)
- D. Security Identifier (SID)

Answer: A

NEW QUESTION 10

You are preparing to start the qualitative risk analysis process for your project. You will be relying on some organizational process assets to influence the process. Which one of the following is NOT a probable reason for relying on organizational process assets as an input for qualitative risk analysis?

- A. Information on prior, similar projects
- B. Review of vendor contracts to examine risks in past projects
- C. Risk databases that may be available from industry sources
- D. Studies of similar projects by risk specialists

Answer: B

NEW QUESTION 13

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 15

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

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

Answer: B

NEW QUESTION 16

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 18

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 23

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 24

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 create an overall project rating scheme to reflect the bias towards risks that affect the project schedule.
- C. She can filter all risks based on their affect on schedule versus other project objectives.
- D. She can shift risk-laden activities that affect the project schedule from the critical path as much as possible.

Answer: B

NEW QUESTION 25

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 30

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 34

You are the project manager for the NHH project. You are working with your project team to examine the project from four different defined perspectives to increase the breadth of identified risks by including internally generated risks. What risk identification approach are you using in this example?

- A. SWOT analysis
- B. Root cause analysis
- C. Assumptions analysis
- D. Influence diagramming techniques

Answer: A

NEW QUESTION 35

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 38

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 39

A project team member has just identified a new project risk. The risk event is determined to have significant impact but a low probability in the project. Should the risk event happen it'll cause the project to be delayed by three weeks, which will cause new risk in the project. What should the project manager do with the risk event?

- A. Add the identified risk to a quality control management control chart.
- B. Add the identified risk to the risk register.
- C. Add the identified risk to the issues log.
- D. Add the identified risk to the low-level risk watchlist.

Answer: B

NEW QUESTION 40

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 43

You work as the project manager for Bluewell Inc. You are working on NGQQ Project you're your company. You have completed the risk analysis processes for the risk events. You and the project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transference
- D. Risk mitigation

Answer: C

NEW QUESTION 45

You work as a project manager for BlueWell Inc. Management has asked you to work with the key project stakeholder to analyze the risk events you have identified in the project. They would like you to analyze the project risks with a goal of improving the project's performance as a whole. What approach can you use to achieve the goal of improving the project's performance through risk analysis with your project stakeholders?

- A. Involve subject matter experts in the risk analysis activities
- B. Focus on the high-priority risks through qualitative risk analysis
- C. Use qualitative risk analysis to quickly assess the probability and impact of risk events
- D. Involve the stakeholders for risk identification only in the phases where the project directly affects them

Answer: B

NEW QUESTION 48

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 49

Which of the following is the acronym of RTM?

- A. Resource tracking method
- B. Requirements Traceability Matrix
- C. Resource timing method
- D. Requirements Testing Matrix

Answer: B

NEW QUESTION 51

Which of the following are the tasks performed by the owner in the information classification schemes?
Each correct answer represents a part of the solution. Choose three.

- A. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
- B. To perform data restoration from the backups whenever required.
- C. To review the classification assignments from time to time and make alterations as the business requirements alter.
- D. To delegate the responsibility of the data safeguard duties to the custodian.

Answer: ACD

NEW QUESTION 52

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

Answer: A

NEW QUESTION 54

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 57

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 59

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 60

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 65

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

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

Answer: A

NEW QUESTION 66

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 69

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 70

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 73

Which of the following is NOT a phase of the security certification and accreditation process?

- A. Initiation
- B. Security certification
- C. Operation
- D. Maintenance

Answer: C

NEW QUESTION 77

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 79

Which of the following processes is used to protect the data based on its secrecy, sensitivity, or confidentiality?

- A. Change Control
- B. Data Hiding
- C. Configuration Management
- D. Data Classification

Answer: D

NEW QUESTION 80

Which of the following components ensures that risks are examined for all new proposed change requests in the change control system?

- A. Risk monitoring and control
- B. Scope change control
- C. Configuration management
- D. Integrated change control

Answer: D

NEW QUESTION 81

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 85

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 90

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 92

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 97

The phase 0 of Risk Management Framework (RMF) is known as strategic risk assessment planning. Which of the following processes take place in phase 0?

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

- A. Review documentation and technical data.
- B. Apply classification criteria to rank data assets and related IT resources.
- C. Establish criteria that will be used to classify and rank data assets.
- D. Identify threats, vulnerabilities, and controls that will be evaluated.
- E. Establish criteria that will be used to evaluate threats, vulnerabilities, and controls.

Answer: BCDE

NEW QUESTION 101

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 102

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 104

Kelly is the project manager of the BHH project for her organization. She is completing the risk identification process for this portion of her project. Which one of the following is the only thing that the risk identification process will create for Kelly?

- A. Project document updates
- B. Risk register updates
- C. Change requests
- D. Risk register

Answer: D

NEW QUESTION 109

You are the project manager for your organization. You are working with your project team to complete the qualitative risk analysis process. The first tool and technique you are using requires that you assess the probability and what other characteristic of each identified risk in the project?

- A. Risk owner
- B. Risk category
- C. Impact
- D. Cost

Answer: C

NEW QUESTION 114

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 116

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 117

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 121

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 122

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

Answer: ABC

NEW QUESTION 126

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 127

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 131

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 132

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 136

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 141

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 142

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 147

Your organization has named you the project manager of the JKN Project. This project has a BAC of \$1,500,000 and it is expected to last 18 months. Management has agreed that if the schedule baseline has a variance of more than five percent then you will need to crash the project. What happens when the project manager crashes a project?

- A. Project costs will increase.
- B. The amount of hours a resource can be used will diminish.
- C. The project will take longer to complete, but risks will diminish.
- D. Project risks will increase.

Answer: A

NEW QUESTION 150

Which of the following individuals makes the final accreditation decision?

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

Answer: B

NEW QUESTION 152

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 153

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 155

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 159

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 161

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 166

Which of the following tasks are identified by the Plan of Action and Milestones document?
Each correct answer represents a complete solution. Choose all that apply.

- A. The plans that need to be implemented
- B. The resources needed to accomplish the elements of the plan
- C. Any milestones that are needed in meeting the tasks
- D. The tasks that are required to be accomplished
- E. Scheduled completion dates for the milestones

Answer: BCDE

NEW QUESTION 169

You are the project manager of the BlueStar 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 qualitative risk analysis process. What will you need as inputs for the qualitative risk analysis of the project in this scenario?

- A. You will need the risk register, risk management plan, project scope statement, 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, permission from the functional manager, and any relevant organizational process assets.
- D. Qualitative risk analysis does not happen through the project manager in a functional structure.

Answer: A

NEW QUESTION 173

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 174

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 175

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 178

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 179

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

Answer: D

NEW QUESTION 181

You are the project manager of QSL project for your organization. You are working with your project team and several key stakeholders to create a diagram that shows how various elements of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?

- A. Cause and effect diagrams
- B. System or process flowcharts
- C. Predecessor and successor diagramming
- D. Influence diagrams

Answer: B

NEW QUESTION 182

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

Answer: ACD

NEW QUESTION 186

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 188

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 190

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 191

Which of the following individuals is responsible for preparing and submitting security status reports to the organizations?

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

Answer: C

NEW QUESTION 195

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

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

Answer: C

NEW QUESTION 198

Which of the following individuals makes the final accreditation decision?

- A. DAA
- B. ISSO
- C. CIO
- D. CISO

Answer: A

NEW QUESTION 201

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 204

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 209

Which of the following guidance documents is useful in determining the impact level of a particular threat on agency systems?

- A. NIST SP 800-41
- B. NIST SP 800-37
- C. FIPS 199
- D. NIST SP 800-14

Answer: C

NEW QUESTION 212

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 214

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 termination clause of the contract stipulates

Answer: D

NEW QUESTION 218

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 219

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

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

Answer: B

NEW QUESTION 224

.....

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](#)