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
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 3
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 4
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 5
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 6
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 7
Management wants you to create a visual diagram of what resources will be utilized in the project deliverables. What type of a chart is management asking you to create?

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

Answer: B

NEW QUESTION 8
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 9
Frank is the project manager of the NHH Project. He is working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document is Frank and the NHH Project team creating in this scenario?

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

Answer: C

NEW QUESTION 10
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 10
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 11
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 12
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. RTM
B. CRO
C. DAA
D. ATM

Answer: A

NEW QUESTION 14

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 16
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 19
You are the project manager for a construction project. The project includes a work that involves very high financial risks. You decide to insure processes so that any ill happening can be compensated. Which type of strategies have you used to deal with the risks involved with that particular work?

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

Answer: A

NEW QUESTION 20
Which of the following are included in Administrative Controls?
Each correct answer represents a complete solution. Choose all that apply.

A. Conducting security-awareness training
B. Screening of personnel
C. Monitoring for intrusion
D. Implementing change control procedures
E. Developing policy

Answer: ABDE

NEW QUESTION 23
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 24
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 29
You are the project manager of the NKQ project for your organization. You have completed the quantitative risk analysis process for this portion of the project. What is the only output of the quantitative risk analysis process?

A. Probability of reaching project objectives
B. Risk contingency reserve
C. Risk response
D. Risk register updates

Answer: D

NEW QUESTION 34
You work as a project manager for BlueWell Inc. You are currently working with the project stakeholders to identify risks in your project. You understand that the qualitative risk assessment and analysis can reflect the attitude of the project team and other stakeholders to risk. Effective assessment of risk requires management of the risk attitudes of the participants. What should you, the project manager, do with assessment of identified risks in consideration of the attitude and bias of the participants towards the project risk?

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

Answer: D

NEW QUESTION 37
Your project is an agricultural-based project that deals with plant irrigation systems. You have discovered a byproduct in your project that your organization could use to make a profityou??re your organization seizes this opportunity it would be an example of what risk response?

A. Opportunistic
B. Positive
C. Enhancing
D. Exploiting

Answer: D

NEW QUESTION 42
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 43
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. Procurement management plan
C. Stakeholder register
D. Quality management plan

Answer: B

NEW QUESTION 44
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 48
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 49
You are the project manager of the GGG project. You have completed the risk identification process for the initial phases of your project. As you begin to document the risk events in the risk register what additional information can you associate with the identified risk events?

A. Risk schedule
B. Risk potential responses

C. Risk cost
D. Risk owner

Answer: B

NEW QUESTION 52
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 56
Mary is the project manager for the BLB project. She has instructed the project team to assemble, to review the risks. She has included the schedule management plan as an input for the quantitative risk analysis process. Why is the schedule management plan needed for quantitative risk analysis?

A. Mary will utilize the schedule controls and the nature of the schedule for the quantitative analysis of the schedule.
B. Mary will schedule when the identified risks are likely to happen and affect the project schedule.
C. Mary will utilize the schedule controls to determine how risks may be allowed to change the project schedule.
D. Mary will use the schedule management plan to schedule the risk identification meetings throughout the remaining project.

Answer: A

NEW QUESTION 59
Which of the following objectives are defined by integrity in the C.I.A triad of information security systems?
Each correct answer represents a part of the solution. Choose three.

A. It preserves the internal and external consistency of information.
B. It prevents the unauthorized or unintentional modification of information by the authorized users.
C. It prevents the intentional or unintentional unauthorized disclosure of a message's contents .
D. It prevents the modification of information by the unauthorized users.

Answer: ABD

NEW QUESTION 60
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 61
In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

A. Full operational test
B. Penetration test
C. Paper test
D. Walk-through test

Answer: B

NEW QUESTION 62
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 studies of similar projects by risk specialists.
B. You will use organizational process assets to determine costs of all risks events within the current project.
C. You will use organizational process assets for information from prior similar projects.
D. You will use organizational process assets for risk databases that may be available from industry sources.

Answer: B

NEW QUESTION 66
Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk

event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

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

Answer: C

NEW QUESTION 71
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 73
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 75
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 3
C. Level 5
D. Level 4
E. Level 1

Answer: B

NEW QUESTION 80
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 82
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 85
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 88
Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

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

Answer: B

NEW QUESTION 89
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABDEFG

NEW QUESTION 91
Which of the following phases begins with a review of the SSAA in the DITSCAP accreditation?

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

Answer: C

NEW QUESTION 94
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 95
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 98
Which of the following relations correctly describes residual risk?

A. Residual Risk = Threats x Vulnerability x Asset Gap x Control Gap
B. Residual Risk = Threats x Exploit x Asset Value x Control Gap
C. Residual Risk = Threats x Exploit x Asset Value x Control Gap
D. Residual Risk = Threats x Vulnerability x Asset Value x Control Gap

Answer: D

NEW QUESTION 102
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 104
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 108
Which of the following assessment methods is used to review, inspect, and analyze assessment objects?

A. Testing
B. Examination
C. Interview
D. Debugging

Answer: B

NEW QUESTION 110
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 111
Ned is the program manager for his organization and he's considering some new materials for his program. He and his team have never worked with these materials before and he wants to ask the vendor for some additional information, a demon, and even some samples. What type of a document should Ned send to the vendor?

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

Answer: B

NEW QUESTION 112
Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

A. Secret information
B. Top Secret information
C. Confidential information
D. Unclassified information

Answer: B

NEW QUESTION 113
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 116
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 monthin the 18-month project.

Answer: A

NEW QUESTION 119
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 122
You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks.
Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

A. A qualitative risk analysis requires fast and simple data to complete the analysis.
B. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.
C. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.
D. A qualitative risk analysis encourages biased data to reveal risk tolerances.

Answer: B

NEW QUESTION 126
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 131
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 133
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 136
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
Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

A. Safeguard
B. Single Loss Expectancy (SLE)
C. Exposure Factor (EF)
D. Annualized Rate of Occurrence (ARO)

Answer: D

NEW QUESTION 139
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 141
Which of the following are the types of access controls?
Each correct answer represents a complete solution. Choose three.

A. Administrative
B. Automatic
C. Technical
D. Physical

Answer: ACD

NEW QUESTION 145
What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?

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

Answer: D

NEW QUESTION 148
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 152
Which of the following documents is described in the statement below?
"It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."

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

Answer: C

NEW QUESTION 156
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 161

What NIACAP certification levels are recommended by the certifier?
Each correct answer represents a complete solution. Choose all that apply.

A. Minimum Analysis
B. Basic System Review
C. Detailed Analysis
D. Maximum Analysis
E. Comprehensive Analysis
F. Basic Security Review

Answer: ACEF

NEW QUESTION 164
You are the project manager for TTP project. You are in the Identify Risks process. You have to create the risk register. Which of the following are included in the risk register?
Each correct answer represents a complete solution. Choose two.

A. List of potential responses
B. List of identified risks
C. List ofmitigation techniques
D. List of key stakeholders

Answer: AB

NEW QUESTION 168
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. Which of the following participants are required in a NIACAP security assessment?
Each correct answer represents a part of the solution. Choose all that apply.

A. Information Assurance Manager
B. Designated Approving Authority
C. IS program manager
D. User representative
E. Certification agent

Answer: BCDE

NEW QUESTION 169
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 174
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 177
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 178
You work as a project manager for TechSoft Inc. You are working with the project stakeholders onthe qualitative risk analysis process in your project. You have

used all the tools to the qualitative risk analysis process in your project. Which of the following techniques is NOT used as a tool in qualitative risk analysis process?

A. Risk Reassessment
B. Risk Categorization
C. Risk Urgency Assessment
D. Risk Data Quality Assessment

Answer: A

NEW QUESTION 180
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 183
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 187
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 andmodeling techniques
B. Data gathering and representation techniques
C. Expert judgment
D. Organizational process assets

Answer: D

NEW QUESTION 191
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 192
Which types of project tends to have more well-understood risks?

A. State-of-art technologyprojects
B. Recurrent projects
C. Operational work projects
D. First-of-its kind technology projects

Answer: B

NEW QUESTION 196
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 197
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 199
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 counterme asure
B. Identifying the risk
C. Assessing the impact of potential threats
D. Identifying the accused

Answer: ABC

NEW QUESTION 203
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 probabilityand impact matrixes
D. Risk identification

Answer: A

NEW QUESTION 205
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 206
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 209
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 212
Certification and Accreditation (C&A or CnA) is a process for implementing information security.
Which of the following is the correct order of C&A phases in a DITSCAP assessment?

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

Answer:

C

NEW QUESTION 214
There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

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

Answer: D

NEW QUESTION 216
Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

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

Answer: B

NEW QUESTION 219
Which of the following assessment methods involves observing or conducting the operation of physical devices?

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

Answer: D

NEW QUESTION 224
Which of the following individuals is responsible for the final accreditation decision?

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

Answer: C

NEW QUESTION 226
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 230
Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

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

Answer: E

NEW QUESTION 231
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 233

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 238
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 243
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. Assumption
B. Issue
C. Risk
D. Constraint

Answer: A

NEW QUESTION 245
Which one of the following is the only output for the qualitative risk analysis process?

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

Answer: C

NEW QUESTION 250
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. Risks
B. Human resource needs
C. Quality control concerns
D. Costs

Answer: A

NEW QUESTION 254
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 256
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 257
A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 258
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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 FirstTry

* CAP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year