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

Answer: C

NEW QUESTION 3
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan?
Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: ABDE

NEW QUESTION 4
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 riskis always in the future.

Answer: D

NEW QUESTION 5
Where can a project manager find risk-rating rules?

A. Risk probability and impact matrix
B. Organizational process assets
C. Enterprise environmental factors
D. Risk management plan

Answer: B

NEW QUESTION 6
Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?

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

Answer: D

NEW QUESTION 7
You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

A. Quantitative risk analysis
B. Qualitative risk analysis

C. Requested changes
D. Risk audits

Answer: C

NEW QUESTION 8

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 9

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

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

Answer: C

NEW QUESTION 10

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 10

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

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

Answer: ABDE

NEW QUESTION 12

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 17

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 19

Gary is the project manager for his project. He and the project team have completed the qualitative risk analysis process and are about to enter the quantitative risk analysis process when

Mary, the project sponsor, wants to know what quantitative risk analysis will review. Which of the following statements best defines what quantitative risk analysis will review?

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

Answer: D

NEW QUESTION 20
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 21
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 25
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 29
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 preservesthe internal and external consistency of information.
B. It prevents the unauthorized or unintentional modification of information by the authorized users.
C. It prevents the modification of information by the unauthorized users.
D. It prevents the intentional or unintentional unauthorized disclosure of a message's contents .

Answer: ABC

NEW QUESTION 30
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 35
Sam is the project manager of a construction project in south Florida. This area of the United States is prone to hurricanes during certain parts of the year. As part of the project plan Sam and the project team acknowledge the possibility of hurricanes and the damage the hurricane could have on the project's deliverables, the schedule of the project, and the overall cost of the project.
Once Sam and the project stakeholders acknowledge the risk of the hurricane they go on planning the project as if the risk is not likely to happen. What type of risk response is Sam using?

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

Answer: C

NEW QUESTION 38
Jeff, a key stakeholder in your project, wants to know how the risk exposure for the risk events is calculated during quantitative risk analysis. He is worried about the risk exposure which is too low for the events surrounding his project requirements. How is the risk exposure calculated?

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

Answer: C

NEW QUESTION 42
You work as a project manager for SoftTech Inc. You are working with the project stakeholders to begin the qualitative risk analysis process. You will need all of the following as inputs to the qualitative risk analysis process except for which one?

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

Answer: C

NEW QUESTION 45
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 48
Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

A. Circumstantial
B. Incontrovertible
C. Direct
D. Corroborating

Answer: A

NEW QUESTION 52
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 55
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 57
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 59
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 61
Which of the following approaches can be used to build a security program?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: AC

NEW QUESTION 66
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 70
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 71
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 72
The Project Risk Management knowledge area focuses on which of the following processes?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 77
Which of the following are the goals of risk management?

Each correct answer represents a complete solution. Choose three.

A. Finding an economic balance between the impact of the risk and the cost of the countermeasure
B. Identifying the risk
C. Assessing the impact of potential threats
D. Identifying the accused

Answer: ABC

NEW QUESTION 79

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 84

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 88

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 89

The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABDE

NEW QUESTION 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 95

Which of the following documents were developed by NIST for conducting Certification & Accreditation (C&A)?
Each correct answer represents a complete solution. Choose all that apply.

A. NIST Special Publication 800-53A
B. NIST Special Publication 800-37A
C. NIST Special Publication 800-59
D. NIST Special Publication 800-53
E. NIST Special Publication 800-37

F. NIST Special Publication 800-60

Answer: ACDEF

NEW QUESTION 97
John is the project manager of the NHQ Project for his company. His project has 75 stakeholders, some of which are external to the organization. John needs to make certain that he communicates about risk in the most appropriate method for the external stakeholders. Which project management plan will be the best guide for John to communicate to the external stakeholders?

A. Communications Management Plan
B. Risk Management Plan
C. Project Management Plan
D. Risk ResponsePlan

Answer: A

NEW QUESTION 100
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 103
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 104
Which of the following formulas was developed by FIPS 199 for categorization of an information type?

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

Answer: B

NEW QUESTION 105
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 108
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 110
Which of the following is not a part of Identify Risks process?

A. System or process flow chart
B. Influence diagram

C. Decision tree diagram
D. Cause and effect diagram

Answer: C

NEW QUESTION 112
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 116
Beth is the project manager of the BFG Project for her company. In this project Beth has decided to create a contingency response based on the performance of the project schedule. If the project schedule variance is greater than $10,000 the contingency plan will be implemented. What is the formula for the schedule variance?

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

Answer: A

NEW QUESTION 120
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 121
Which of the following is used in the practice of Information Assurance (IA) to define assurance requirements?

A. Classic information security model
B. Communications Management Plan
C. Five Pillars model
D. Parkerian Hexad

Answer: A

NEW QUESTION 124
Which of the following describes residual risk as the risk remaining after risk mitigation has occurred?

A. DIACAP
B. ISSO
C. SSAA
D. DAA

Answer: A

NEW QUESTION 127
Which of the following individuals is responsible for monitoring the information system environment for factors that can negatively impact the security of the system and its accreditation?

A. Chief Risk Officer
B. Chief Information Security Officer
C. Information System Owner
D. Chief Information Officer

Answer: C

NEW QUESTION 131
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 management plan
B. Project contractual relationship with the vendor
C. Project communications plan
D. Project scope statement

Answer: A

NEW QUESTION 134
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 139
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 140
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 142
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 147
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 148
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 151
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 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 157
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 158
Information Security management is a process of defining the security controls in order to protect information assets. What are the security management responsibilities?
Each correct answer represents a complete solution. Choose all that apply.

A. Evaluating business objectives, security risks, user productivity, and functionality requirem ents
B. Determining actual goals that are expected to be accomplished from a security program
C. Defining steps to ensure that all the responsibilities are accounted for and properly address ed
D. Determining objectives, scope, policies, priorities, standards, and strategies

Answer: ABCD

NEW QUESTION 163
Which of the following are included in Technical Controls?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABCDF

NEW QUESTION 167
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 172
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 177
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 182
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 185
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 189
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 192
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 196
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Network security policy
B. User password policy
C. Backup policy
D. Privacy policy

Answer: D

NEW QUESTION 199
ISO 17799 has two parts. The first part is an implementation guide with guidelines on how to build a comprehensive information security infrastructure and the second part is an auditing guide based on requirements that must be met for an organization to be deemed compliant with ISO 17799. What are the ISO 17799 domains?
Each correct answer represents a complete solution. Choose all that apply.

A. Information security policy for the organization
B. System architecture management
C. Business continuity management
D. System developmentand maintenance
E. Personnel security

Answer: ACDE

NEW QUESTION 200
The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. What are the process activities of this phase?
Each correct answer represents a complete solution. Choose all that apply.

A. Perform certification evaluation of the integrated system
B. System development
C. Certification and accreditation decision
D. Develop recommendation to the DAA
E. Continue to review and refine the SSAA

Answer: ACDE

NEW QUESTION 205
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. Risk Response Plan
B. Risk Management Plan
C. Project ManagementPlan
D. Communications Management Plan

Answer: D

NEW QUESTION 209
Which of the following individuals makes the final accreditation decision?

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

Answer: B

NEW QUESTION 212
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 216
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 ISSO manages the security of the information system that is slated for Certification &Accreditation (C&A).
B. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
C. An ISSE provides advice on the continuous monitoring of the information system.
D. An ISSO takes part in the development activities that are required to implement system ch anges.
E. An ISSE provides advice on the impacts of system changes.

Answer: ACE

NEW QUESTION 220
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 224
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 225
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 230
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 231
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. Avoidance
B. Acceptance
C. Transference
D. Mitigation

Answer: A

NEW QUESTION 232
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 234
You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

A. Qualitative risk analysis
B. Seven risk responses
C. Quantitative risk analysis
D. A risk probability-impact matrix

Answer: A

NEW QUESTION 238
Which of the following statements about role-based access control (RBAC) model is true?

A. In this model, the permissions are uniquely assigned to each user account.
B. In this model, a user can access resources according to his role in the organization.
C. In this model, the same permission is assigned to each user account.
D. In this model, the users canaccess resources according to their seniority.

Answer: B

NEW QUESTION 239
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 243
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 246
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

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

Answer: B

NEW QUESTION 249
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 253
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 256
According to FIPS Publication 199, what are the three levels of potential impact on organizations in the event of a compromise on confidentiality, integrity, and availability?

A. Confidential, Secret, and High
B. Minimum, Moderate, and High
C. Low, Normal, and High
D. Low, Moderate, and High

Answer: D

NEW QUESTION 259

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 261
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 266
In which of the following phases does the change management process start?

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

Answer: C

NEW QUESTION 269
Which of the following individuals is responsible for configuration management and control task?

A. Authorizing official
B. Information system owner
C. Chief information officer
D. Common control provider

Answer: B

NEW QUESTION 271
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 276
Which of the following is used throughout the entire C&A process?

A. DAA
B. DITSCAP
C. SSAA
D. DIACAP

Answer: C

NEW QUESTION 281
In which of the following elements of security does the object retain its veracity and is intentionally modified by the authorized subjects?

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

Answer: A

NEW QUESTION 285
Which of the following recovery plans includes a monitoring process and triggers for initiating planned actions?

A. Business continuity plan
B. Contingency plan
C. Continuity of Operations Plan

D. Disaster recovery plan

Answer: B

NEW QUESTION 290
Which of the following individuals makes the final accreditation decision?

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

Answer: A

NEW QUESTION 292
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 294
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 297
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 300
Management wants you to create a visual diagram of what resources will be utilized in the project deliverables. What type of a chart is management asking you to create?

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

Answer: C

NEW QUESTION 304
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 306
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 307
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 312
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 315
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 316
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 321
During which of the following processes, probability and impact matrix is prepared?

A. Plan Risk Responses
B. Perform Quantitative Risk Analysis
C. Perform Qualitative Risk Analysis
D. Monitoring and Control Risks

Answer: C

NEW QUESTION 323
Which of the following statements about Discretionary Access Control List (DACL) is true?

A. It is a rule list containing access control entries.
B. It specifies whether an audit activity should be performed when an object attempts to access a resource.
C. It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.
D. It is a unique number that identifies a user, group, and computer account

Answer: C

NEW QUESTION 325
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 328
Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

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

Answer: A

NEW QUESTION 330
......

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

100% Actual & Verified — Instant Download, Please Click
Order The CAP Practice Test Here