ISC2

Exam Questions CAP

ISC2 CAP Certified Authorization Professional

NEW QUESTION 1
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. Common Control Provider
D. Chief Information Officer

Answer: C

NEW QUESTION 2
Which of the following assessment methodologies defines a six-step technical security evaluation?

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

Answer: B

NEW QUESTION 3
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 4
Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

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

Answer: B

NEW QUESTION 5
James work as an IT systems personnel in SoftTech Inc. He performs the following tasks: Runs regular backups and routine tests of the validity of the backup data.
Performs data restoration from the backups whenever required.
Maintains the retained records in accordance with the established information classification policy.
What is the role played by James in the organization?

A. Manager
B. Owner
C. Custodian
D. User

Answer: C

NEW QUESTION 6
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 7
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. Verification, Validation, Definition, and Post Accreditation
D. Definition, Verification, Validation, and Post Accreditation

Answer: D

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

Answer: ABDE

NEW QUESTION 9
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 10
The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 10
DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP?
Each correct answer represents a complete solution. Choose all that apply.

A. Validation
B. Re-Accreditation
C. Verification
D. System Definition
E. Identification
F. Accreditation

Answer: ABCD

NEW QUESTION 14
The phase 3 of the Risk Management Framework (RMF) process is known as mitigation planning.
Which of the following processes take place in phase 3?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 16
Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. What are the different categories of risk?
Each correct answer represents a complete solution. Choose all that apply.

A. System interaction
B. Human interaction

C. Equipment malfunction
D. Inside and outside attacks
E. Social status
F. Physical damage

Answer: BCDEF

NEW QUESTION 21
In which type of access control do user ID and password system come under?

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

Answer: B

NEW QUESTION 26
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 31
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 32
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 35
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 39
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 43
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 47
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 49
Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

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

Answer: A

NEW QUESTION 50
Which of the following are included in Physical Controls?
Each correct answer represents a complete solution. Choose all that apply.

A. Locking systems and removing unnecessary floppy or CD-ROM drives
B. Environmental controls
C. Password and resource management
D. Identification and authentication methods
E. Monitoring for intrusion
F. Controlling individual access into the facilityand different departments

Answer: ABEF

NEW QUESTION 53
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 55
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 60
Eric is the project manager of the MTC project for his company. In this project a vendor has offered Eric a sizeable discount on all hardware if his order total for the project is more than $125,000. Right now, Eric is likely to spend $118,000 with vendor. If Eric spends $7,000 his cost savings for the project will be $12,500, but he cannot purchase hardware if he cannot implement the hardware immediately due to organizational policies. Eric consults with Amy and Allen, other project managers in the organization, and asks if she needs any hardware for their projects. Both Amy and Allen need hardware and they agree to purchase the hardware through Eric's relationship with the vendor. What positive risk response has happened in this instance?

A. Transference
B. Exploiting
C. Sharing

D. Enhancing

Answer: C

NEW QUESTION 62
You work as a project manager for BlueWell Inc. You are preparing to plan risk responses for your project with your team. How many risk response types are available for a negative risk event in the project?

A. Seven
B. Three
C. Four
D. One

Answer: C

NEW QUESTION 67
You are the project manager of the GHQ project for your company. You are working you??re your project team to prepare for the qualitative risk analysis process. Mary, a project team member, does not understand why you need to complete qualitative risks analysis. You explain to Mary that qualitative risks analysis helps you determine which risks needs additional analysis. There are also some other benefits that qualitative risks analysis can do for the project. Which one of the following is NOT an accomplishment of the qualitative risk analysis process?

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

Answer: A

NEW QUESTION 69
What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Configuration Management System
B. Project Management InformationSystem
C. Scope Verification
D. Integrated Change Control

Answer: A

NEW QUESTION 71
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 74
During qualitative risk analysis you want to define the risk urgency assessment. All of the following are indicators of risk priority except for which one?

A. Risk rating
B. Warning signs
C. Cost of the project
D. Symptoms

Answer: C

NEW QUESTION 77
You work as the project manager for Bluewell Inc. You are working on NGQQ Projectyou??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 78
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 80
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 83
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 86
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 87
What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

A. PON
B. ZOPA
C. BATNA
D. Bias

Answer: C

NEW QUESTION 92
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 96
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 98
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 100
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 101
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 103
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 107
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 109
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 111
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 113
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. DC Security Design & Configuration
B. VI Vulnerability and Incident Management
C. EC Enclave and Computing Environment
D. Information systems acquisition, development, and maintenance

Answer: ABC

NEW QUESTION 117
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 119
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 120
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. Personnel security
C. Business continuity management
D. System architecture management
E. System development and maintenance

Answer: ABCE

NEW QUESTION 123
Joan is a project management consultant and she has been hired by a firm to help them identify risk events within the project. Joan would first like to examine the project documents including the plans, assumptions lists, project files, and contracts. What key thing will help Joan to discover risks within the review of the project documents?

A. Lack of consistency between the plans and the project requirements and assumptions can bethe indicators of risk in the project.
B. The project documents will help the project manager, or Joan, to identify what risk identification approach is best to pursue.
C. Plans that have loose definitions of terms and disconnected approaches will revealrisks.
D. Poorly written requirements will reveal inconsistencies in the project plans and documents.

Answer: A

NEW QUESTION 128
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 130
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 process will analyze the effect of risk events that may substantially impact the project's competing demands.
B. The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.
C. The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.
D. 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.

Answer: A

NEW QUESTION 134
You are the project manager of the NNH Project. In this project you have created a contingency response that the schedule performance index should be less than 0.93. The NHH Project has a budget at completion of $945,000 and is 45 percent complete though the project should be 49 percent complete. The project has spent $455,897 to reach the 45 percent complete milestone.
What is the project's schedule performance index?

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

Answer: D

NEW QUESTION 136
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 137
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 142
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 144
You are the project manager of the HJK Project for your organization. You and the project team have created risk responses for many of the risk events in the project. Where should you document the proposed responses and the current status of all identified risks?

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

Answer: C

NEW QUESTION 146
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 147
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 152
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 156
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 160
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 161
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 163
Which of the following statements about the availability concept of Information security management is true?

A. It ensures that modifications are not made to data by unauthorized personnel or processes .
B. It ensures reliable and timely access to resources.
C. It determines actions and behaviors of a single individual within a system.
D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Answer: B

NEW QUESTION 165
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 168
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 173
Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing?
Each correct answer represents a complete solution. Choose all that apply.

A. Full-box
B. Zero-knowledge test
C. Full-knowledge test
D. Open-box
E. Partial-knowledge test
F. Closed-box

Answer: BCDEF

NEW QUESTION 175
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 180
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 181
You are the project manager of the GHY Project for your company. You have completed the risk response planning with your project team. You now need to update the WBS. Why would the project manager need to update the WBS after the risk response planning process? Choose the best answer.

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

Answer: D

NEW QUESTION 185
Which of the following is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold?

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

Answer: C

NEW QUESTION 187
Gary is the project manager for his organization. He is working with the project stakeholders on the project requirements and how risks may affect their project. One of the stakeholders is confused about what constitutes risks in the project. Which of the following is the most accurate definition of a project risk?

A. It is an uncertain event that can affect the project costs.
B. It is an uncertain event or condition within the project execution.
C. It is an uncertain event that can affect at least one project objective.
D. It is an unknown event that can affect the project scope.

Answer: C

NEW QUESTION 188
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 193
You are the project manager for your organization. You have determined that an activity is too dangerous to complete internally so you hire licensed contractor to complete the work. The contractor, however, may not complete the assigned work on time which could cause delays in subsequent work beginning. This is an example of what type of risk event?

A. Secondary risk
B. Transference
C. Internal
D. Pure risk

Answer: A

NEW QUESTION 198
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 200
David is the project manager of HGF project for his company. David, the project team, and several key stakeholders have completed risk identification and are ready to move into qualitative risk analysis. Tracy, a project team member, does not understand why they need to complete qualitative risk analysis. Which one of the following is the best explanation for completing qualitative risk analysis?

A. It isa rapid and cost-effective means of establishing priorities for the plan risk responses and lays the foundation for quantitative analysis.
B. It is a cost-effective means of establishing probability and impact for the project risks.
C. Qualitative risk analysis helps segment the project risks, create a risk breakdown structure, and create fast and accurate risk responses.
D. All risks must pass through quantitative risk analysis before qualitative risk analysis.

Answer: A

NEW QUESTION 205
An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

A. Anonymous
B. Multi-factor
C. Biometrics
D. Mutual

Answer: B

NEW QUESTION 209
Which of the following risk responses delineates that the project plan will not be changed to deal with the risk?

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

Answer: A

NEW QUESTION 214
Which of the following individuals makes the final accreditation decision?

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

Answer: B

NEW QUESTION 215
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 218
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 221
Mark works as a project manager for TechSoft Inc. Mark, the project team, and the key project stakeholders have completed a round of qualitative risk analysis. He needs to update the risk register with his findings so that he can communicate the risk results to the project stakeholders - including management. Mark will need to update all of the following information except for which one?

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

Answer: B

NEW QUESTION 223
Jenny is the project manager for the NBT projects. She is working with the project team and several subject matter experts to perform the quantitative risk analysis process. During this process she and the project team uncover several risks events that were not previously identified.
What should Jenny do with these risk events?

A. The events should be determined if they need to be accepted or responded to.
B. The events should be entered into qualitative risk analysis.
C. The events should continue on with quantitative risk analysis.
D. The events should be entered into the risk register.

Answer: D

NEW QUESTION 227
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 232
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 234
Which of the following acts promote a risk-based policy for cost effective security?
Each correct answer represents a part of the solution. Choose all that apply.

A. Clinger-Cohen Act
B. Lanham Act
C. Computer Misuse Act
D. Paperwork Reduction Act (PRA)

Answer: AD

NEW QUESTION 239
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 244
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. Certification is a comprehensive assessment of the management, operational, and technical security controls inan information system.
C. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
D. Certification is the official management decision given by a senior agency official to authorize operation of an information system.

Answer: AB

NEW QUESTION 245
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 248
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 253
Which of the following parts of BS 7799 covers risk analysis and management?

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

Answer: B

NEW QUESTION 255
Which of the following NIST documents includes components for penetration testing?

A. NIST SP 800-53

B. NIST SP 800-26
C. NIST SP 800-37
D. NIST SP 800-30

Answer: D

NEW QUESTION 260
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 262
In which of the following phases do the system security plan update and the Plan of Action and Milestones (POAM) update take place?

A. Continuous Monitoring Phase
B. Accreditation Phase
C. Preparation Phase
D. DITSCAP Phase

Answer: A

NEW QUESTION 267
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 272
Which of the following NIST publications defines impact?

A. NIST SP 800-41
B. NIST SP 800-37
C. NIST SP 800-30
D. NIST SP 800-53

Answer: C

NEW QUESTION 273
Which of the following relations correctly describes total risk?

A. Total Risk = Threats x Vulnerability x Asset Value
B. Total Risk = Viruses x Vulnerability x Asset Value
C. Total Risk = Threats x Exploit x Asset Value
D. Total Risk = Viruses x Exploit x Asset Value

Answer: A

NEW QUESTION 274
Which of the following individuals makes the final accreditation decision?

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

Answer: A

NEW QUESTION 277
Which of the following are the types of assessment tests addressed in NIST SP 800-53A?

A. Functional, penetration, validation
B. Validation, evaluation, penetration
C. Validation, penetration, evaluation
D. Functional, structural, penetration

Answer: D

NEW QUESTION 281
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 286
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 289
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 293
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 295
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 299
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 300
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 305
Which of the following statements correctly describes DIACAP residual risk?

A. It is the remaining risk to the information system after risk palliation has occurred.
B. It is a process of security authorization.
C. It is the technical implementation of the security design.
D. It is used to validate the information system.

Answer: A

NEW QUESTION 306
......