Exam Questions CAP

ISC2 CAP Certified Authorization Professional

https://www.2passeasy.com/dumps/CAP/

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

Answer: ACD

NEW QUESTION 3
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 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
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 6
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. User
C. Owner
D. Custodian

Answer: D

NEW QUESTION 7
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 8
Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

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

Answer: B

NEW QUESTION 9
In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

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

Answer: B

NEW QUESTION 10
You are the project manager of the NHH project for your company. You have completed the first round of risk management planning and have created four outputs of the risk response planning process. Which one of the following is NOT an output of the risk response planning?

A. Risk-related contract decisions
B. Project document updates
C. Risk register updates
D. Organizational process assets updates

Answer: D

NEW QUESTION 10
Jenny is the project manager of the NHJ Project for her company. She has identified several positive risk events within the project and she thinks these events can save the project time and money. You, a new team member wants to know that how many risk responses are available for a positive risk event. What will Jenny reply to you?

A. Four
B. Seven
C. Acceptance is the only risk response for positive risk events.
D. Three

Answer: A

NEW QUESTION 11
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 15
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 16
Fred is the project manager of the PKL project. He is working with his project team to complete the quantitative risk analysis process as a part of risk management planning. Fred understands that once the quantitative risk analysis process is complete, the process will need to be completed again in at least two other times in the project. When will the quantitative risk analysis process need to be repeated?

A. Quantitative risk analysisprocess will be completed again after the plan risk response planning and as part of procurement.
B. Quantitative risk analysis process will be completed again after the cost managementplanning and as a part of monitoring and controlling.
C. Quantitativerisk analysis process will be completed again after new risks are identified and as part of monitoring and controlling.
D. Quantitative risk analysis process will be completed again after the risk response planning and as a part of monitoring and controlling.

Answer: D

NEW QUESTION 17
The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABCD

NEW QUESTION 18
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 22
To help review or design security controls, they can be classified by several criteria. One of these criteria is based on nature. According to this criteria, which of the following controls consists of incident response processes, management oversight, security awareness, and training?

A. Technical control
B. Physical control
C. Procedural control
D. Compliance control

Answer: C

NEW QUESTION 24
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 27
A project team member has just identified a new project risk. The risk event is determined to have significant impact but a low probability in the project. Should the risk event happen it'll cause the project to be delayed by three weeks, which will cause new risk in the project. What should the project manager do with the risk event?

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

Answer: B

NEW QUESTION 32
Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

A. Chief Information Security Officer
B. Senior Management
C. Information Security Steering Committee
D. Business Unit Manager

Answer: B

NEW QUESTION 33
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 34
Courtney is the project manager for her organization. She is working with the project team to complete the qualitative risk analysis for her project. During the analysis Courtney encourages the project team to begin the grouping of identified risks by common causes. What is the primary advantage to group risks by common causes during qualitative risk analysis?

A. It can lead to developing effective risk responses.
B. It can lead to the creation of risk categories unique to each project.
C. It helps the project team realize the areas of the project most laden with risks.
D. It saves time by collecting the related resources, such as project team members, to analyze the risk events.

Answer: A

NEW QUESTION 37
You work as a project manager for BlueWell Inc. You are working with Nancy, the COO of your company, on several risks within the project. Nancy understands that through qualitative analysis you have identified 80 risks that have a low probability and low impact as the project is currently planned. Nancy's concern, however, is that the impact and probability of these risk events may change as conditions within the project may change. She would like to know where will you document and record these 80 risks that have low probability and low impact for future reference.
What should you tell Nancy?

A. Risk identification is an iterative process so any changes to the low probability and low impact risks will be reassessed throughout the project life cycle.
B. Risks with low probability and low impact are recorded in a watchlist for future monitoring.
C. All risks, regardless of their assessed impact and probability, are recorded in the risk log.
D. All risks are recorded in the risk management plan

Answer: B

NEW QUESTION 40
Thomas is the project manager of the NHJ Project for his company. He has identified several positive risk events within his project and he thinks these events can save the project time and money. Positive risk events, such as these within the NHJ Project are also known as what?

A. Opportunities
B. Benefits
C. Ancillary constituent components
D. Contingency risks

Answer: A

NEW QUESTION 45
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 50
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 52
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 57
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 59
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. Teamingagreements
B. Crashing the project
C. Transference
D. Fast tracking the project

Answer: B

NEW QUESTION 64
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 65
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

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

Answer: C

NEW QUESTION 68
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 72
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. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
B. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
C. Certification isthe official management decision given by a senior agency official to authorize operation of an information system.
D. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.

Answer: AD

NEW QUESTION 74
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 78
Your project has several risks that may cause serious financial impact should they happen. You have studied the risk events and made some potential risk responses for the risk events but management wants you to do more. They'd like for you to create some type of a chart that identified the risk probability and impact with a financial amount for each risk event. What is the likely outcome of creating this type of chart?

A. Quantitative analysis
B. Risk response plan
C. Contingency reserve
D. Risk response

Answer: C

NEW QUESTION 79
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 82
Which of the following is NOT an objective of the security program?

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

Answer: A

NEW QUESTION 84
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABDEFG

NEW QUESTION 85
Harry is the project manager of the MMQ Construction Project. In this project Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States. Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project's deadline. Management asked Harry to find a supplier who will guarantee the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?

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

Answer: A

NEW QUESTION 88
In which of the following Risk Management Framework (RMF) phases is strategic risk assessment planning performed?

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

Answer: A

NEW QUESTION 90
Which of the following is NOT a type of penetration test?

A. Cursory test
B. Partial-knowledge test
C. Zero-knowledge test
D. Full knowledge test

Answer: A

NEW QUESTION 93
Which of the following relations correctly describes residual risk?

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

Answer: D

NEW QUESTION 97
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 99
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 103
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 104
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 106
Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

A. Computer Fraud and Abuse Act
B. FISMA
C. Lanham Act
D. Computer Misuse Act

Answer: B

NEW QUESTION 111
Which of the following access control models uses a predefined set of access privileges for an object of a system?

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

Answer: B

NEW QUESTION 114
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 119
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 120
Fill in the blank with an appropriate word.
________ ensures that the information is not disclosed to unauthorized persons or processes.

A. Confidentiality

Answer: A

NEW QUESTION 125
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 127
The only output of the perform qualitative risk analysis are risk register updates. When the project manager updates the risk register he will need to include several pieces of information including all of the following except for which one?

A. Trends in qualitative risk analysis
B. Risk probability-impact matrix
C. Watchlist of low-priority risks
D. Risks grouped by categories

Answer: B

NEW QUESTION 130
Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?

A. At every status meeting the project team project risk management is an agenda item.
B. Project risk management happens at every milestone.
C. Project risk management has been concluded with the project planning.
D. Project risk management is scheduled for every monthin the 18-month project.

Answer: A

NEW QUESTION 133
You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?

A. Risk management plan
B. Enterprise environmental factors
C. Staffing management plan
D. Risk register

Answer: A

NEW QUESTION 137
In which of the following DIACAP phases is residual risk analyzed?

A. Phase 2
B. Phase 4
C. Phase 5
D. Phase 3
E. Phase 1

Answer: B

NEW QUESTION 139
You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

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

Answer: A

NEW QUESTION 144
A high-profile, high-priority project within your organization is being created. Management wants you to pay special attention to the project risks and do all that you can to ensure that all of the risks are identified early in the project. Management has to ensure that this project succeeds.
Management's risk aversion in this project is associated with what term?

A. Utility function
B. Risk conscience
C. Quantitativerisk analysis
D. Risk mitigation

Answer: A

NEW QUESTION 146
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

A. Configuration management
B. Procurement management
C. Risk management
D. Change management

Answer: A

NEW QUESTION 148
Who is responsible for the stakeholder expectations management in a high-profile, high-risk project?

A. Project management office
B. Project sponsor
C. Project risk assessment officer
D. Project manager

Answer: D

NEW QUESTION 150
Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event?

A. Corrective action
B. Technical performance measurement
C. Risk audit
D. Earned value management

Answer: A

NEW QUESTION 155
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 157
Which of the following statements about System Access Control List (SACL) is true?

A. It contains a list of any events that are set to audit for that particular object.
B. It is a mechanism for reducing the need for globally unique IP addresses.
C. It contains a list of both users and groups and whatever permissions they have.
D. It exists for each and every permission entry assigned to any object.

Answer: A

NEW QUESTION 158
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 161
What NIACAP certification levels are recommended by the certifier?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACEF

NEW QUESTION 162
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 165
You are the project manager for TTP project. You are in the Identify Risks process. You have to create the risk register. Which of the following are included in the risk register?
Each correct answer represents a complete solution. Choose two.

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

D. List of key stakeholders

Answer: AB

NEW QUESTION 170
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 175
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 178
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 180
You work as a project manager for BlueWell Inc. You are working with your team members on the risk responses in the project. Which risk response will likely cause a project to use the procurement processes?

A. Acceptance
B. Mitigation
C. Exploiting
D. Sharing

Answer: D

NEW QUESTION 183
Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 187
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 190
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 192
Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

A. It depends on what the outcome of a lawsuit will determine.
B. No, the ZAS Corporation did not complete all of the work.
C. It depends on what the termination clause of the contract stipulates.
D. Yes, the ZAS Corporation did not choose to terminate the contract work.

Answer: C

NEW QUESTION 197
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 202
Which of the following tasks are identified by the Plan of Action and Milestones document?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCDE

NEW QUESTION 203
Harry is the project manager of the MMQ Construction Project. In this project Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States. Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project's deadline. Management asked Harry to find a supplier who will guarantee the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?

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

Answer: B

NEW QUESTION 206
Which of the following are the goals of risk management?
Each correct answer represents a complete solution. Choose three.

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

Answer: ABC

NEW QUESTION 207
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 212
You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

A. It is a risk that remains because no risk response is taken.
B. It is a risk that remains after planned risk responses are taken.
C. It is a risk that can not be addressed by a risk response.
D. It is a risk that will remain no matter what type of risk response is offered.

Answer: B

NEW QUESTION 214
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 217
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 222
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 223
NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews?

A. Substantial
B. Significant
C. Abbreviated
D. Comprehensive

Answer: C

NEW QUESTION 228
What are the responsibilities of a system owner?
Each correct answer represents a complete solution. Choose all that apply.

A. Integrates security considerations into application and system purchasing decisions and development projects.
B. Ensures that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.
C. Ensures that adequate security is being provided by the necessary controls, password management, remoteaccess controls, operating system configurations, and so on.
D. Ensures that the necessary security controls are in place.

Answer: ABC

NEW QUESTION 229
Which of the following groups represents the most likely source of an asset loss through the inappropriate use of computers?

A. Hackers

B. Visitors
C. Customers
D. Employees

Answer: D

NEW QUESTION 234
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 240
Certification and Accreditation (C&A or CnA) is a process for implementing information security.
Which of the following is the correct order of C&A phases in a DITSCAP assessment?

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

Answer: C

NEW QUESTION 245
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 248
Which of the following system security policies is used to address specific issues of concern to the organization?

A. Program policy
B. Issue-specific policy
C. Informative policy
D. System-specific policy

Answer: B

NEW QUESTION 253
Which of the following individuals is responsible for ensuring the security posture of the organization's information system?

A. Authorizing Official
B. Chief Information Officer
C. Security Control Assessor
D. Common Control Provider

Answer: A

NEW QUESTION 258
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 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 262
Which of the following assessment methods involves observing or conducting the operation of physical devices?

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

Answer: D

NEW QUESTION 265
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 267
Which of the following is used throughout the entire C&A process?

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

Answer: C

NEW QUESTION 270
Which of the following C&A professionals plays the role of an advisor?

A. Information System Security Engineer (ISSE)
B. Chief Information Officer (CIO)
C. Authorizing Official
D. Information Owner

Answer: A

NEW QUESTION 275
Which of the following formulas was developed by FIPS 199 for categorization of an information system?

A. SCinformation system = {(confidentiality, impact), (integrity, controls), (availability, risk)}
B. SCinformation system = {(confidentiality, risk), (integrity, impact), (availability, controls)}
C. SCinformation system = {(confidentiality, impact), (integrity, impact), (availability, impact)}
D. SCinformation system = {(confidentiality, controls), (integrity, controls), (availability, controls)}

Answer: C

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 280
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 283
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 288
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 289
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 290
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. Symptoms
B. Cost of the project
C. Warning signs
D. Risk rating

Answer: B

NEW QUESTION 291
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 296
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 300

......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAP Product From:

https://www.2passeasy.com/dumps/CAP/

Money Back Guarantee

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