

## CAP Dumps

### ISC2 CAP Certified Authorization Professional

<https://www.certleader.com/CAP-dumps.html>



#### 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

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 4

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

**Answer:** D

#### NEW QUESTION 5

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 6

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 7

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

- A. Risk response plan
- B. Quantitative analysis
- C. Risk response

D. Contingency reserve

**Answer:** D

**NEW QUESTION 8**

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 9**

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 10**

Gary is the project manager of his organization. He is managing a project that is similar to a project his organization completed recently. Gary has decided that he will use the information from the past project to help him and the project team to identify the risks that may be present in the project. Management agrees that this checklist approach is ideal and will save time in the project.

Which of the following statement is most accurate about the limitations of the checklist analysis approach for Gary?

- A. The checklist analysis approach is fast but it is impossible to build an exhaustive checklist.
- B. The checklist analysis approach only uses qualitative analysis.
- C. The checklist analysis approach saves time, but can cost more.
- D. The checklist is also known as top down risk assessment

**Answer:** A

**NEW QUESTION 10**

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 14**

You and your project team are identifying the risks that may exist within your project. Some of the risks are small risks that won't affect your project much if they happen. What should you do with these identified risk events?

- A. These risks can be accepted.
- B. These risks can be added to a low priority risk watch list.
- C. All risks must have a valid, documented risk response.
- D. These risks can be dismissed.

**Answer:** B

**NEW QUESTION 19**

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

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

**Answer:** A

**NEW QUESTION 20**

You are the project manager for your organization. You have identified a risk event you??re your organization could manage internally or externally. If you manage the event internally it will cost your project \$578,000 and an additional \$12,000 per month the solution is in use. A vendor can manage the risk event for you. The vendor will charge \$550,000 and \$14,500 per month that the solution is in use. How many months will you need to use the solution to pay for the internal solution in comparison to the vendor's solution?

- A. Approximately 13 months
- B. Approximately 11 months
- C. Approximately 15 months
- D. Approximately 8 months

**Answer:** B

#### NEW QUESTION 25

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 27

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

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

**Answer:** C

#### NEW QUESTION 29

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 31

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

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

**Answer:** D

#### NEW QUESTION 35

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 NNH 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. 0.92
- C. -\$37,800
- D. 0.93

**Answer:** B

#### NEW QUESTION 40

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 43

You are the project manager for your company and a new change request has been approved for your project. This change request, however, has introduced several new risks to the project. You have communicated these risk events and the project stakeholders understand the possible effects these risks could have on your project. You elect to create a mitigation response for the identified risk events. Where will you record the mitigation response?

- A. Project management plan
- B. Risk management plan
- C. Risk log
- D. Risk register

**Answer:** D

#### NEW QUESTION 48

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 51

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 56

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 facility and different departments

**Answer:** ABEF

#### NEW QUESTION 57

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 58

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

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

**Answer:** B

#### NEW QUESTION 59

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 60

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 61

You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

- A. Sharing
- B. Avoidance
- C. Transference
- D. Exploiting

**Answer:** C

#### NEW QUESTION 66

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 71

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 74

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 77

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 79

Your organization has a project that is expected to last 20 months but the customer would really like the project completed in 18 months. You have worked on similar projects in the past and believe that you could fast track the project and reach the 18 month deadline. What increases when you fast track a project?

- A. Risks
- B. Costs
- C. Resources
- D. Communication

**Answer:** A

#### NEW QUESTION 82

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

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

**Answer:** D

#### NEW QUESTION 86

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 89

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

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

**Answer:** D

#### NEW QUESTION 90

You are the program manager for your project. You are working with the project managers regarding the procurement processes for their projects. You have ruled out one particular contract type because it is considered too risky for the program. Which one of the following contract types is usually considered to be the most dangerous for the buyer?

- A. Cost plus incentive fee
- B. Time and materials
- C. Cost plus percentage of costs
- D. Fixed fee

**Answer:** C

#### NEW QUESTION 92

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 94

There are seven risk 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 95

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 96

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

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

**Answer:** B

#### NEW QUESTION 99

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 103

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

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

**Answer:** B

#### NEW QUESTION 104

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 is the 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 107

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 be the 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 reveal risks.
- D. Poorly written requirements will reveal inconsistencies in the project plans and documents.

**Answer:** A



**NEW QUESTION 108**

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 113**

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 116**

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 120**

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 121**

Which of the following is NOT a responsibility of a data owner?

- A. Maintaining and protecting data
- B. Ensuring that the necessary security controls are in place
- C. Delegating responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian
- D. Approving access requests

**Answer:** A

**NEW QUESTION 124**

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 129**

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 131**

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 132**

Which of the following administrative policy controls requires individuals or organizations to be engaged in good business practices relative to the organization's industry?

- A. Segregation of duties
- B. Separation of duties
- C. Need to Know
- D. Due care

**Answer:** D

**NEW QUESTION 136**

Which of the following is a security policy implemented by an organization due to compliance, regulation, or other legal requirements?

- A. Advisory policy
- B. Informative policy
- C. System Security policy
- D. Regulatory policy

**Answer:** D

**NEW QUESTION 139**

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 144**

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 148**

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 151**

In which of the following phases does the SSAA maintenance take place?

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

**Answer:** D

**NEW QUESTION 154**

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 158**

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 162**

You are the project manager for your organization. You are working with your key stakeholders in the qualitative risk analysis process. You understand that there is certain bias towards the risk events in the project that you need to address, manage, and ideally reduce. What solution does the PMBOK recommend to reduce the influence of bias during qualitative risk analysis?

- A. Establish the definitions of the levels of probability and impact
- B. Isolate the stakeholders by project phases to determine their risk bias
- C. Involve all stakeholders to vote on the probability and impact of the risk events
- D. Provide iterations of risk analysis for true reflection of a risk probability and impact

**Answer:** A

**NEW QUESTION 165**

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 170**

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 174**

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 175**

You work as the project manager for Bluewell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decide, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project, what is likely to increase?

- A. Human resource needs
- B. Risks
- C. Costs
- D. Quality control concerns

**Answer:** B

**NEW QUESTION 177**

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

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

**Answer:** B

**NEW QUESTION 181**

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. Contingent response strategy
- B. Expert judgment
- C. Internal risk management strategy
- D. External risk response

**Answer:** A

**NEW QUESTION 185**

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 188**

Nancy is the project manager of the NHH project. She and the project team have identified a significant risk in the project during the qualitative risk analysis process. Bob is familiar with the technology that the risk is affecting and proposes to Nancy a solution to the risk event. Nancy tells Bob that she has noted his response, but the risk really needs to pass through the quantitative risk analysis process before creating responses. Bob disagrees and ensures Nancy that his response is most appropriate for the identified risk. Who is correct in this scenario?

- A. Bob is correc
- B. Bob is familiar with the technology and the risk event so his response should be implemented.
- C. Nancy is correc
- D. Because Nancy is the project manager she can determine the correct procedures for risk analysis and risk response
- E. In addition, she has noted the risk response that Bob recommends.
- F. Nancy is correc
- G. All risks of significant probability and impact should pass the quantitative risk analysis process before risk responses are created.
- H. Bob is correc
- I. Not all riskevents have to pass the quantitative risk analysis process to develop effective risk responses.

**Answer:** D

**NEW QUESTION 192**

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase?

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

- A. Maintenance of the SSAA
- B. Compliance validation
- C. Change management
- D. System operations
- E. Security operations
- F. Continue to review and refine the SSAA

**Answer:** ABCDE

**NEW QUESTION 195**

You are the project manager of a large construction project. Part of the project involves the wiring of the electricity in the building your project is creating. You and the project team determine the electrical work is too dangerous to perform yourself so you hire an electrician to perform the work for the project. This is an example of what type of risk response?

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

**Answer:** A

**NEW QUESTION 200**

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 201**

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. Quantitative risk analysis
- D. Risk mitigation

**Answer:** A

**NEW QUESTION 203**

What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Conduct activities related to the disposition of the system data and objects.
- B. Execute and update IA implementation plan.
- C. Conduct validation activities.
- D. Combine validation results in DIACAP scorecard.

**Answer:** BCD

**NEW QUESTION 207**

The phase 0 of Risk Management Framework (RMF) is known as strategic risk assessment planning. Which of the following processes take place in phase 0?  
Each correct answer represents a complete solution. Choose all that apply.

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

**Answer:** BCDE

**NEW QUESTION 208**

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 209**

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 212**

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

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

**Answer:** D

**NEW QUESTION 215**

Which of the following documents is described in the statement below?

"It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."

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

**Answer:** C

**NEW QUESTION 216**

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 217**

Which of the following are the objectives of the security certification documentation task?

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

- A. To prepare the Plan of Action and Milestones (POAM) based on the security assessment
- B. To provide the certification findings and recommendations to the information system owner
- C. To assemble the final security accreditation package and then submit it to the authorizing official
- D. To update the system security plan based on the results of the security assessment

**Answer:** ABCD

**NEW QUESTION 220**

You are preparing to complete the quantitative risk analysis process with your project team and several subject matter experts. You gather the necessary inputs including the project's cost management plan. Why is it necessary to include the project's cost management plan in the preparation for the quantitative risk analysis process?

- A. The project's cost management plan can help you to determine what the total cost of the project is allowed to be.
- B. The project's cost management plan provides direction on how costs may be changed due to identified risks.
- C. The project's cost management plan provides control that may help determine the structure for quantitative analysis of the budget.
- D. The project's cost management plan is not an input to the quantitative risk analysis process .

**Answer:** C

**NEW QUESTION 224**

You work as a project manager for BlueWell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decided, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project which of the following are likely to increase?

- A. Quality control concerns
- B. Costs
- C. Risks
- D. Human resource needs

**Answer:** C

**NEW QUESTION 226**

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 231**

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 233

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 of mitigation techniques
- D. List of key stakeholders

**Answer:** AB

#### NEW QUESTION 234

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. Which of the following participants are required in a NIACAP security assessment?

Each correct answer represents a part of the solution. Choose all that apply.

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

**Answer:** BCDE

#### NEW QUESTION 238

BS 7799 is an internationally recognized ISM standard that provides high level, conceptual recommendations on enterprise security. BS 7799 is basically divided into three parts. Which of the following statements are true about BS 7799?

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

- A. BS 7799 Part 1 was adopted by ISO as ISO/IEC 27001 in November 2005.
- B. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.
- C. BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards Institute (BSI) in 1995.
- D. BS 7799 Part 3 was published in 2005, covering risk analysis and management.

**Answer:** BCD

#### NEW QUESTION 242

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 246

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 247

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 and modeling techniques
- B. Data gathering and representation techniques
- C. Expert judgment
- D. Organizational process assets

**Answer:** D

**NEW QUESTION 248**

You work as a project manager for TechSoft Inc. You, the project team, and the key project stakeholders have completed a round of quantitative risk analysis. You now need to update the risk register with your findings so that you can communicate the risk results to the project stakeholders - including management. You will need to update all of the following information except for which one?

- A. Probability of achieving cost and time objectives
- B. Risk distributions within the project schedule
- C. Probabilistic analysis of the project
- D. Trends in quantitative risk analysis

**Answer:** B

**NEW QUESTION 252**

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 255**

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 260**

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 261**

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 263**

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 268**

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

- A. Authenticity
- B. Confidentiality
- C. Availability
- D. Integrity

**Answer:** B

#### NEW QUESTION 271

Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. For what purposes is ST&E used? Each correct answer represents a complete solution. Choose all that apply.

- A. To implement the design of system architecture
- B. To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
- C. To assess the degree of consistency between the system documentation and its implementation
- D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

**Answer:** BCD

#### NEW QUESTION 276

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 277

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 279

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 281

In what portion of a project are risk and opportunities greatest and require intense planning and anticipation of risk events?

- A. Planning
- B. Executing
- C. Closing
- D. Initiating

**Answer:** D

#### NEW QUESTION 285

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 289**

Ned is the project manager of the HNN project for your company. Ned has asked you to help him complete some probability distributions for his project. What portion of the project will you most likely use for probability distributions?

- A. Uncertainty in values such as duration of schedule activities
- B. Bias towards risk in new resources
- C. Risk probability and impact matrixes
- D. Risk identification

**Answer:** A

**NEW QUESTION 291**

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 293**

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 298**

You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?

- A. Risk identification
- B. Qualitative risk analysis
- C. Risk response implementation
- D. Quantitative risk analysis

**Answer:** D

**NEW QUESTION 299**

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 303**

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 308**

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

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

**Answer:** C

**NEW QUESTION 310**

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 314**

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 316**

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 321**

What does OCTAVE stand for?

- A. Operationally Computer Threat, Asset, and Vulnerability Evaluation
- B. Operationally Critical Threat, Asset, and Vulnerability Evaluation
- C. Operationally Computer Threat, Asset, and Vulnerability Elimination
- D. Operationally Critical Threat, Asset, and Vulnerability Elimination

**Answer:** B

**NEW QUESTION 324**

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 327**

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 328**

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 332**

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

- A. Certification Agent
- B. User Representative

- C. Information System Owner
- D. Risk Executive

**Answer:** C

#### NEW QUESTION 337

Which of the following individuals makes the final accreditation decision?

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

**Answer:** A

#### NEW QUESTION 338

Tom is the project manager for his organization. In his project he has recently finished the risk response planning. He tells his manager that he will now need to update the cost and schedule baselines. Why would the risk response planning cause Tom the need to update the cost and schedule baselines?

- A. New or omitted work as part of a risk response can cause changes to the cost and/or schedule baseline.
- B. Risk responses protect the time and investment of the project.
- C. Risk responses may take time and money to implement.
- D. Baselines should not be updated, but refined through versions.

**Answer:** A

#### NEW QUESTION 341

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 342

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

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

**Answer:** D

#### NEW QUESTION 344

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 347

Which of the following processes is described in the statement below?

"It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

- A. Perform Quantitative Risk Analysis
- B. Monitor and Control Risks
- C. Perform Qualitative Risk Analysis
- D. Identify Risks

**Answer:** B

#### NEW QUESTION 350

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

**Answer:** CDE

**NEW QUESTION 351**

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

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

**Answer:** B

**NEW QUESTION 356**

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

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

**Answer:** B

**NEW QUESTION 358**

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 360**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your CAP Exam with Our Prep Materials Via below:**

<https://www.certleader.com/CAP-dumps.html>