

CAP Dumps

ISC2 CAP Certified Authorization Professional

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



NEW QUESTION 1

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 2

The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE?

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

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

Answer: ACE

NEW QUESTION 3

System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan?

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

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

Answer: ABDE

NEW QUESTION 4

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation?

Each correct answer represents a complete solution. Choose two.

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

Answer: AD

NEW QUESTION 5

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 6

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation?

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

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

Answer: BCD

NEW QUESTION 7

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 8

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 9

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

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

Answer: B

NEW QUESTION 10

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 10

Adrian is the project manager of the NHP Project. In her project there are several work packages that deal with electrical wiring. Rather than to manage the risk internally she has decided to hire a vendor to complete all work packages that deal with the electrical wiring. By removing the risk internally to a licensed electrician Adrian feels more comfortable with project team being safe.
What type of risk response has Adrian used in this example?

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

Answer: B

NEW QUESTION 15

You are preparing to start the qualitative risk analysis process for your project. You will be relying on some organizational process assets to influence the process. Which one of the following is NOT a probable reason for relying on organizational process assets as an input for qualitative risk analysis?

- A. Information on prior, similar projects
- B. Review of vendor contracts to examine risks in past projects
- C. Risk databases that may be available from industry sources
- D. Studies of similar projects by risk specialists

Answer: B

NEW QUESTION 19

A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

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

Answer: D

NEW QUESTION 21

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

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

Answer: ABCDEG

NEW QUESTION 22

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. Walk-through test
- C. Penetration test
- D. Paper test

Answer: C

NEW QUESTION 24

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 26

Which of the following roles is also known as the accreditor?

- A. Chief Risk Officer
- B. Data owner
- C. Designated Approving Authority
- D. Chief Information Officer

Answer: C

NEW QUESTION 30

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 34

Thomas is a key stakeholder in your project. Thomas has requested several changes to the project scope for the project you are managing. Upon review of the proposed changes, you have discovered that these new requirements are laden with risks and you recommend to the change control board that the changes be excluded from the project scope. The change control board agrees with you. What component of the change control system communicates the approval or denial of a proposed change request?

- A. Configuration management system
- B. Change log
- C. Scope change control system
- D. Integrated change control

Answer: D

NEW QUESTION 37

A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

- A. Security law
- B. Privacy law
- C. Copyright law
- D. Trademark law

Answer: B

NEW QUESTION 39

Which of the following is a 1996 United States federal law, designed to improve the way the federal government acquires, uses, and disposes information technology?

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

Answer: C

NEW QUESTION 43

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 44

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

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

Answer: A

NEW QUESTION 46

Amy is the project manager for her company. In her current project the organization has a very low tolerance for risk events that will affect the project schedule. Management has asked Amy to consider the affect of all the risks on the project schedule. What approach can Amy take to create a bias against risks that will affect the schedule of the project?

- A. She can have the project team pad their time estimates to alleviate delays in the project schedule.
- B. She can create an overall project rating scheme to reflect the bias towards risks that affect the project schedule.
- C. She can filter all risks based on their affect on schedule versus other project objectives.
- D. She can shift risk-laden activities that affect the project schedule from the critical path as much as possible.

Answer: B

NEW QUESTION 48

Which of the following processes is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

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

Answer: B

NEW QUESTION 50

Wendy is about to perform qualitative risk analysis on the identified risks within her project. Which one of the following will NOT help Wendy to perform this project management activity?

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

Answer: A

NEW QUESTION 53

Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

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

Answer: A

NEW QUESTION 58

You are the project manager of the GHG project. You are preparing for the quantitative risk analysis process. You are using organizational process assets to help you complete the quantitative risk analysis process. Which one of the following is NOT a valid reason to utilize organizational process assets as a part of the quantitative risk analysis process?

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

Answer: C

NEW QUESTION 63

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

- A. It preserves the internal and external consistency of information.
- B. It prevents the unauthorized or unintentional modification of information by the authorized users.
- C. It prevents the 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 67

You and your project team are just starting the risk identification activities for a project that is scheduled to last for 18 months. Your project team has already identified a long list of risks that need to be analyzed. How often should you and the project team do risk identification?

- A. At least once per month
- B. Identify risks is an iterative process.
- C. It depends on how many risks are initially identified.
- D. Several times until the project moves into execution

Answer: B

NEW QUESTION 68

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

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

Answer: ABDE

NEW QUESTION 71

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 73

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 78

Which of the following are the common roles with regard to data in an information classification program?
Each correct answer represents a complete solution. Choose all that apply.

- A. Custodian
- B. User
- C. Security auditor
- D. Editor
- E. Owner

Answer: ABCE

NEW QUESTION 83

An Authorizing Official plays the role of an approver. What are the responsibilities of an Authorizing Official?
Each correct answer represents a complete solution. Choose all that apply.

- A. Establishing and implementing the organization's continuous monitoring program
- B. Determining the requirement of reauthorization and reauthorizing information systems when required
- C. Reviewing security status reports and critical security documents
- D. Ascertaining the security posture of the organization's information system

Answer: BCD

NEW QUESTION 85

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

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

Answer: C

NEW QUESTION 88

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 91

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 93

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 97

The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA?
Each correct answer represents a complete solution. Choose all that apply.

- A. IATO
- B. ATO

- C. IATT
- D. ATT
- E. DATO

Answer: ABCE

NEW QUESTION 99

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. Baselines should not be updated, but refined through versions.
- D. Risk responses may take time and money to implement.

Answer: A

NEW QUESTION 103

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

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

Answer: D

NEW QUESTION 108

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 111

You work as a project manager for BlueWell Inc. Management has asked you to work with the key project stakeholder to analyze the risk events you have identified in the project. They would like you to analyze the project risks with a goal of improving the project's performance as a whole. What approach can you use to achieve the goal of improving the project's performance through risk analysis with your project stakeholders?

- A. Involve subject matter experts in the risk analysis activities
- B. Focus on the high-priority risks through qualitative risk analysis
- C. Use qualitative risk analysis to quickly assess the probability and impact of risk events
- D. Involve the stakeholders for risk identification only in the phases where the project directly affects them

Answer: B

NEW QUESTION 116

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 119

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 124

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 129

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 132

Which of the following statements is true about residual risks?

- A. It is a weakness or lack of safeguard that can be exploited by a threat.
- B. It can be considered as an indicator of threats coupled with vulnerability.
- C. It is the probabilistic risk after implementing all security measures.
- D. It is the probabilistic risk before implementing all security measures.

Answer: C

NEW QUESTION 134

Your project uses a piece of equipment that if the temperature of the machine goes above 450 degree Fahrenheit the machine will overheat and have to be shut down for 48 hours. Should this machine overheat even once it will delay the project's end date. You work with your project to create a response that should the temperature of the machine reach 430, the machine will be paused for at least an hour to cool it down. The temperature of 430 is called what?

- A. Risk identification
- B. Risk response
- C. Risk trigger
- D. Risk event

Answer: C

NEW QUESTION 139

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 140

Which of the following is an Information Assurance (IA) model that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation?

- A. Parkerian Hexad
- B. Capability Maturity Model (CMM)
- C. Classic information security model
- D. Five Pillars model

Answer: D

NEW QUESTION 142

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. Teaming agreements
- B. Crashing the project
- C. Transference
- D. Fast tracking the project

Answer: B

NEW QUESTION 146

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 147

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 148

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 150

Amy is the project manager for her company. In her current project the organization has a very low tolerance for risk events that will affect the project schedule. Management has asked Amy to consider the affect of all the risks on the project schedule. What approach can Amy take to create a bias against risks that will affect the schedule of the project?

- A. She can have the project team pad their time estimates to alleviate delays in the project schedule.
- B. She can shift risk-laden activities that affect the project schedule from the critical path as much as possible.
- C. She can create an overall project rating scheme to reflect the bias towards risks that affect the project schedule.
- D. She can filter all risks based on their affect on schedule versus other project objectives.

Answer: C

NEW QUESTION 154

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 155

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 160

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

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

Answer: A

NEW QUESTION 164

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 166

Gary is the project manager for his project. He and the project team have completed the qualitative risk analysis process and are about to enter the quantitative risk analysis process when Mary, the project sponsor, wants to know what quantitative risk analysis will review. Which of the following statements best defines what quantitative risk analysis will review?

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

Answer: A

NEW QUESTION 171

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 174

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 178

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 181

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 182

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 185

Which of the following is NOT considered an environmental threat source?

- A. Pollution
- B. Hurricane
- C. Chemical
- D. Water

Answer: B

NEW QUESTION 190

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 195

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

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

Answer: B

NEW QUESTION 199

Which of the following NIST documents defines impact?

- A. NIST SP 800-53
- B. NIST SP 800-26
- C. NIST SP 800-30
- D. NIST SP 800-53A

Answer: C

NEW QUESTION 204

Which of the following is NOT a phase of the security certification and accreditation process?

- A. Initiation
- B. Security certification
- C. Operation
- D. Maintenance

Answer: C

NEW QUESTION 207

Which of the following processes has the goal to ensure that any change does not lead to reduced or compromised security?

- A. Change control management
- B. Security management
- C. Configuration management
- D. Risk management

Answer: A

NEW QUESTION 210

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 212

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

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

Answer: A

NEW QUESTION 216

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 220

Which of the following assessment methods is used to review, inspect, and analyze assessment objects?

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

Answer: B

NEW QUESTION 222

Which of the following documents is used to provide a standard approach to the assessment of NIST SP 800-53 security controls?

- A. NIST SP 800-37
- B. NIST SP 800-41
- C. NIST SP 800-53A
- D. NIST SP 800-66

Answer: C

NEW QUESTION 223

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 226

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 228

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 international information security standards? Each correct answer represents a complete solution. Choose all that apply.

- A. Human resources security
- B. Organization of information security
- C. Risk assessment and treatment
- D. AU audit and accountability

Answer: ABC

NEW QUESTION 233

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 236

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 240

Joan is the project manager of the BTT project for her company. She has worked with her project to create risk responses for both positive and negative risk events within the project. As a result of this process Joan needs to update the project document updates. She has updated the assumptions log as a result of the findings and risk responses, but what other documentation will need to be updated as an output of risk response planning?

- A. Lessons learned
- B. Scope statement
- C. Risk Breakdown Structure
- D. Technical documentation

Answer: D

NEW QUESTION 241

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 242

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 244

Which of the following is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls?

- A. IATT
- B. ATO
- C. IATO
- D. DATO

Answer: C

NEW QUESTION 249

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 251

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 month in the 18-month project.

Answer: A

NEW QUESTION 254

You are the project manager of the GGH Project in your company. Your company is structured as a functional organization and you report to the functional manager that you are ready to move onto the quantitative risk analysis process. What things will you need as inputs for the quantitative risk analysis of the project in this scenario?

- A. You will need the risk register, risk management plan, permission from the functional manager, and any relevant organizational process assets.
- B. You will need the risk register, risk management plan, outputs of qualitative risk analysis, and any relevant organizational process assets.
- C. You will need the risk register, risk management plan, cost management plan, schedule management plan, and any relevant organizational process assets.
- D. Quantitative risk analysis does not happen through the project manager in a functional structure.

Answer: C

NEW QUESTION 258

Mark is the project manager of the BFL project for his organization. He and the project team are creating a probability and impact matrix using RAG rating. There is some confusion and disagreement among the project team as to how a certain risk is important and priority for attention should be managed. Where can Mark determine the priority of a risk given its probability and impact?

- A. Risk response plan
- B. Project sponsor
- C. Risk management plan
- D. Look-up table

Answer: D

NEW QUESTION 259

FITSAP stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAP levels shows that the procedures and controls are tested and reviewed?

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

Answer: C

NEW QUESTION 261

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 263

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 266

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 267

Which of the following are the types of access controls?

Each correct answer represents a complete solution. Choose three.

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

Answer: ACD

NEW QUESTION 271

You are the project manager of the NNQ Project for your company and are working you??re your project team to define contingency plans for the risks within your project. Mary, one of your project team members, asks what a contingency plan is. Which of the following statements best defines what a contingency response is?

- A. Some responses are designed for use only if certain events occur.
- B. Some responses have a cost and a time factor to consider for each risk event.
- C. Some responses must counteract pending risk events.
- D. Quantified risks should always have contingency responses.

Answer: A

NEW QUESTION 273

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 275

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 276

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 277

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 280

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 281

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 282

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

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

Answer: BCDEF

NEW QUESTION 285

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 287

The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented?
Each correct answer represents a complete solution. Choose all that apply.

- A. Configuration status accounting
- B. Configuration change control
- C. Configuration deployment
- D. Configuration audits
- E. Configuration identification
- F. Configuration implementation

Answer: ABDE

NEW QUESTION 290

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 292

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 295

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

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

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

Answer: C

NEW QUESTION 298

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

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

Answer: D

NEW QUESTION 300

The risk transference is referred to the transfer of risks to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Which one of the following is NOT an example of the transference risk response?

- A. Use of insurance
- B. Life cycle costing
- C. Warranties
- D. Performance bonds

Answer: B

NEW QUESTION 304

Adrian is a project manager for a new project using a technology that has recently been released and there's relatively little information about the technology. Initial testing of the technology makes the use of it look promising, but there's still uncertainty as to the longevity and reliability of the technology. Adrian wants to consider the technology factors a risk for her project. Where should she document the risks associated with this technology so she can track the risk status and responses?

- A. Project charter
- B. Risk register
- C. Project scope statement
- D. Risk low-level watch list

Answer: B

NEW QUESTION 307

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

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

Answer: C

NEW QUESTION 311

You work as a project manager for TechSoft Inc. You are working with the project stakeholders on the qualitative risk analysis process in your project. You have used all the tools to the qualitative risk analysis process in your project. Which of the following techniques is NOT used as a tool in qualitative risk analysis process?

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

Answer: A

NEW QUESTION 314

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

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

Answer: A

NEW QUESTION 316

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 321

Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives?

- A. NIST SP 800-53A
- B. NIST SP 800-26
- C. NIST SP 800-53
- D. NIST SP 800-59
- E. NIST SP 800-60
- F. NIST SP 800-37

Answer: B

NEW QUESTION 326

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 5
- C. Level 4
- D. Level 1
- E. Level 3

Answer: E

NEW QUESTION 328

Sammy is the project manager for her organization. She would like to rate each risk based on its probability and affect on time, cost, and scope. Harry, a project team member, has never done this before and thinks Sammy is wrong to attempt this approach. Harry says that an accumulative risk score should be created, not three separate risk scores. Who is correct in this scenario?

- A. Harry is correct, because the risk probability and impact considers all objectives of the project.
- B. Harry is correct, the risk probability and impact matrix is the only approach to risk assessment.
- C. Sammy is correct, because she is the project manager.
- D. Sammy is correct, because organizations can create risk scores for each objective of the project.

Answer: D

NEW QUESTION 331

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

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

Answer: B

NEW QUESTION 336

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 339

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 343

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 346

Which of the following individuals makes the final accreditation decision?

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

Answer: B

NEW QUESTION 348

Which of the following DoD directives defines DITSCAP as the standard C&A process for the Department of Defense?

- A. DoD 8000.1
- B. DoD 5200.40
- C. DoD 5200.22-M
- D. DoD 8910.1

Answer: B

NEW QUESTION 351

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 352

Which types of project tends to have more well-understood risks?

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

Answer: B

NEW QUESTION 357

The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE?

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

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

Answer: ACE

NEW QUESTION 358

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?

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

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

Answer: ABC

NEW QUESTION 361

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 362

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 364

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 365

Elizabeth is a project manager for her organization and she finds risk management to be very difficult for her to manage. She asks you, a lead project manager, at what stage in the project will risk management become easier. What answer best resolves the difficulty of risk management practices and the effort required?

- A. Risk management only becomes easier the more often it is practiced.
- B. Risk management is an iterative process and never becomes easier.
- C. Risk management only becomes easier when the project moves into project execution.
- D. Risk management only becomes easier when the project is closed.

Answer: A

NEW QUESTION 368

Which of the following RMF phases identifies key threats and vulnerabilities that could compromise the confidentiality, integrity, and availability of the institutional critical assets?

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

Answer: B

NEW QUESTION 373

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 376

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 381

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 386

You are the project manager for your organization. You are preparing for the quantitative risk analysis. Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?

- A. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.
- B. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
- C. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.
- D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.

Answer: D

NEW QUESTION 389

Fred is the project manager of the CPS project. He is working with his project team to prioritize the identified risks within the CPS project. He and the team are prioritizing risks for further analysis or action by assessing and combining the risks probability of occurrence and impact. What process is Fred completing?

- A. Risk identification
- B. Perform qualitative analysis
- C. Perform quantitative analysis
- D. Risk Breakdown Structure creation

Answer: B

NEW QUESTION 390

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 394

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 395

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 399

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 401

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.

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

Answer: AB

NEW QUESTION 402

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 404

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 405

You are the project manager of QSL project for your organization. You are working with your project team and several key stakeholders to create a diagram that shows how various elements of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?

- A. Cause and effect diagrams
- B. System or process flowcharts
- C. Predecessor and successor diagramming
- D. Influence diagrams

Answer: B

NEW QUESTION 410

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 can access resources according to their seniority.

Answer: B

NEW QUESTION 413

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 417

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 418

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 421

In which of the following Risk Management Framework (RMF) phases is a risk profile created for threats?

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

Answer: C

NEW QUESTION 424

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 429

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 431

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

- A. Confidential, Secret, and High
- B. Minimum, Moderate, and High

- C. Low, Normal, and High
- D. Low, Moderate, and High

Answer: D

NEW QUESTION 435

Which of the following is a risk that is created by the response to another risk?

- A. Secondary risk
- B. Residual risk
- C. Positive risk
- D. Negative risk

Answer: A

NEW QUESTION 438

Which of the following is not a part of Identify Risks process?

- A. Decision tree diagram
- B. Cause and effect diagram
- C. Influence diagram
- D. System or process flow chart

Answer: A

NEW QUESTION 442

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 444

Which of the following statements is true about the continuous monitoring process?

- A. It takes place in the middle of system security accreditation.
- B. It takes place before and after system security accreditation.
- C. It takes place before the initial system security accreditation.
- D. It takes place after the initial system security accreditation.

Answer: D

NEW QUESTION 447

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 448

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 452

Which of the following individuals is responsible for preparing and submitting security status reports to the organizations?

- A. Chief Information Officer
- B. Senior Agency Information Security Officer
- C. Common Control Provider
- D. Authorizing Official

Answer: C

NEW QUESTION 456

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

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

Answer: C

NEW QUESTION 457

Which of the following is used throughout the entire C&A process?

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

Answer: C

NEW QUESTION 462

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

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

Answer: B

NEW QUESTION 466

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 471

A _____ points to a statement in a policy or procedure that helps determine a course of action.

- A. Comment
- B. Guideline
- C. Procedure
- D. Baseline

Answer: B

NEW QUESTION 474

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

- A. Commoncontrol provider
- B. Information system owner
- C. Authorizing official
- D. Chief information officer

Answer: B

NEW QUESTION 477

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 478

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 482

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

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

Answer: C

NEW QUESTION 484

Which of the following RMF phases is known as risk analysis?

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

Answer: C

NEW QUESTION 489

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

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

Answer: A

NEW QUESTION 492

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

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

Answer: B

NEW QUESTION 495

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. Low
- B. Moderate
- C. High
- D. Medium

Answer: ACD

NEW QUESTION 499

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 501

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 505

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 506

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 507

.....

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>