



ISC2

Exam Questions CAP

ISC2 CAP Certified Authorization Professional

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

James work as an IT systems personnel in SoftTech Inc. He performs the following tasks: Runs regular backups and routine tests of the validity of the backup data.

Performs data restoration from the backups whenever required.

Maintains the retained records in accordance with the established information classification policy.

What is the role played by James in the organization?

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

Answer: C

NEW QUESTION 5

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 6

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 7

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 8

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 9

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. VI Vulnerability and Incident Management
- B. DC Security Design & Configuration
- C. EC Enclave and Computing Environment
- D. Information systems acquisition, development, and maintenance

Answer: ABC

NEW QUESTION 10

Ben is the project manager of the YHT Project for his company. Alice, one of his team members, is confused about when project risks will happen in the project. Which one of the following statements is the most accurate about when project risk happens?

- A. Project risk can happen at any moment.
- B. Project risk is uncertain, so no one can predict when the event will happen.
- C. Project risk happens throughout the project execution.
- D. Project risks always in the future.

Answer: D

NEW QUESTION 10

You are the project manager of the NKJ Project for your company. The project's success or failure will have a significant impact on your organization's profitability for the coming year. Management has asked you to identify the risk events and communicate the event's probability and impact as early as possible in the project. Management wants to avoid risk events and needs to analyze the cost-benefits of each risk event in this project. What term is assigned to the low-level of stakeholder tolerance in this project?

- A. Risk avoidance
- B. Mitigation-ready project management
- C. Risk utility function
- D. Risk-reward mentality

Answer: C

NEW QUESTION 15

Where can a project manager find risk-rating rules?

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

Answer: B

NEW QUESTION 17

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 22

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 23

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 25

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 30

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

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

Answer: C

NEW QUESTION 32

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 37

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 38

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 39

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 44

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

- A. Safeguards
- B. Preventive controls
- C. Detective controls
- D. Corrective controls

Answer: D

NEW QUESTION 46

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 50

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 54

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 58

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 61

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 64

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 66

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 71

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 73

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 77

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 81

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

- A. Transference
- B. Exploiting

- C. Sharing
- D. Enhancing

Answer: C

NEW QUESTION 83

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 85

Sam is the project manager of a construction project in south Florida. This area of the United States is prone to hurricanes during certain parts of the year. As part of the project plan Sam and the project team acknowledge the possibility of hurricanes and the damage the hurricane could have on the project's deliverables, the schedule of the project, and the overall cost of the project.

Once Sam and the project stakeholders acknowledge the risk of the hurricane they go on planning the project as if the risk is not likely to happen. What type of risk response is Sam using?

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

Answer: C

NEW QUESTION 88

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

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

Answer: D

NEW QUESTION 93

You are the project manager for a construction project. The project includes a work that involves very high financial risks. You decide to insure processes so that any ill happening can be compensated. Which type of strategies have you used to deal with the risks involved with that particular work?

- A. Transfer
- B. Mitigate
- C. Accept
- D. Avoid

Answer: A

NEW QUESTION 94

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

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

Answer: D

NEW QUESTION 96

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 101

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 105

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 107

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 Information System
- C. Scope Verification
- D. Integrated Change Control

Answer: A

NEW QUESTION 108

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

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

Answer: B

NEW QUESTION 110

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 114

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 118

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 120

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 121

Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

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

Answer: B

NEW QUESTION 126

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 128

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

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

Answer: A

NEW QUESTION 131

You are the project manager of the GGG project. You have completed the risk identification process for the initial phases of your project. As you begin to document the risk events in the risk register what additional information can you associate with the identified risk events?

- A. Risk schedule
- B. Risk potential responses
- C. Risk cost
- D. Risk owner

Answer: B

NEW QUESTION 136

Which of the following are the tasks performed by the owner in the information classification schemes?

Each correct answer represents a part of the solution. Choose three.

- A. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
- B. To perform data restoration from the backups whenever required.
- C. To review the classification assignments from time to time and make alterations as the business requirements alter.
- D. To delegate the responsibility of the data safeguard duties to the custodian.

Answer: ACD

NEW QUESTION 141

Mary is the project manager for the BLB project. She has instructed the project team to assemble, to review the risks. She has included the schedule management plan as an input for the quantitative risk analysis process. Why is the schedule management plan needed for quantitative risk analysis?

- A. Mary will utilize the schedule controls and the nature of the schedule for the quantitative analysis of the schedule.
- B. Mary will schedule when the identified risks are likely to happen and affect the project schedule.
- C. Mary will utilize the schedule controls to determine how risks may be allowed to change the project schedule.
- D. Mary will use the schedule management plan to schedule the risk identification meetings throughout the remaining project.

Answer: A

NEW QUESTION 145

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 146

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

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

Answer: BCD

NEW QUESTION 148

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 149

Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

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

Answer: C

NEW QUESTION 152

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

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

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

Answer: A

NEW QUESTION 155

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 156

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 157

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

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

Answer: A

NEW QUESTION 160

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 165

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 167

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

- A. Safeguards
- B. Preventive controls
- C. Detective controls
- D. Corrective controls

Answer: D

NEW QUESTION 169

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

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

Answer: A

NEW QUESTION 170

Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

- A. Project communications plan
- B. Project management plan
- C. Projectcontractual relationship with the vendor
- D. Project scope statement

Answer: B

NEW QUESTION 175

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

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

Answer: ABDEFG

NEW QUESTION 179

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 180

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 182

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

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

Answer: B

NEW QUESTION 185

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

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

Answer: B

NEW QUESTION 186

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 188

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 191

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 193

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 196

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 198

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

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

Answer: A

NEW QUESTION 203

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

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

Answer: C

NEW QUESTION 205

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 210

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 212

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 215

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 217

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

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

Answer: B

NEW QUESTION 222

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

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

Answer: A

NEW QUESTION 226

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 230

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 232

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 236

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 241

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 246

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 248

The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase?

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

- A. Registration
- B. Document mission need
- C. Negotiation
- D. Initial Certification Analysis

Answer: ABC

NEW QUESTION 251

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 254

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

Which of the following statements are true about security risks?
Each correct answer represents a complete solution. Choose three.

- A. They can be removed completely by taking proper actions.
- B. They can be analyzed and measured by the risk analysis process.
- C. They can be mitigated by reviewing and taking responsible actions based on possible risks.
- D. They are considered an indicator of threats coupled with vulnerability.

Answer: BCD

NEW QUESTION 261

Which of the following governance bodies directs and coordinates implementations of the information security program?

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

Answer: D

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 264

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 266

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Single Loss Expectancy (SLE)
- C. Exposure Factor (EF)
- D. Annualized Rate of Occurrence (ARO)

Answer: D

NEW QUESTION 269

Information Security management is a process of defining the security controls in order to protect information assets. The first action of a management program to implement information security is to have a security program in place. What are the objectives of a security program?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ACD

NEW QUESTION 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 274

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 277

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 279

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 284

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 287

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

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

Answer: A

NEW QUESTION 289

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 294

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 299

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 302

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 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 306

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 308

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 311

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 313

Lisa is the project manager of the SQL project for her company. She has completed the risk response planning with her project team and is now ready to update the risk register to reflect the risk response. Which of the following statements best describes the level of detail Lisa should include with the risk responses she has created?

- A. The level of detail is set by historical information.
- B. The level of detail must define exactly the risk response for each identified risk.
- C. The level of detail is set of project risk governance.
- D. The level of detail should correspond with the priority ranking

Answer: D

NEW QUESTION 314

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

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

Answer: A

NEW QUESTION 315

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

Answer: D

NEW QUESTION 319

An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

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

Answer: D

NEW QUESTION 324

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

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

Answer: D

NEW QUESTION 327

ISO 17799 has two parts. The first part is an implementation guide with guidelines on how to build a comprehensive information security infrastructure and the second part is an auditing guide based on requirements that must be met for an organization to be deemed compliant with ISO 17799. What are the ISO 17799 domains?

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

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

Answer: ACDE

NEW QUESTION 331

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 335

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 338

Your organization has named you the project manager of the JKN Project. This project has a BAC of \$1,500,000 and it is expected to last 18 months. Management has agreed that if the schedule baseline has a variance of more than five percent then you will need to crash the project. What happens when the project manager crashes a project?

- A. Project costs will increase.
- B. The amount of hours a resource can be used will diminish.
- C. The projectwill take longer to complete, but risks will diminish.
- D. Project risks will increase.

Answer: A

NEW QUESTION 341

Which of the following individuals makes the final accreditation decision?

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

Answer: B

NEW QUESTION 344

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 345

Virginia is the project manager for her organization. She has hired a subject matter expert to interview the project stakeholders on certain identified risks within the project. The subject matter expert will assess the risk event with what specific goal in mind?

- A. To determine the bias of the risk event based on each person interviewed
- B. To determine the probability and cost of the risk event
- C. To determine the validity of each risk event
- D. To determine the level of probability and impact for each risk event

Answer: D

NEW QUESTION 347

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. Informative
- C. Regulatory
- D. Advisory

Answer: BCD

NEW QUESTION 352

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

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

Answer: D

NEW QUESTION 355

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 359

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

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

Answer: C

NEW QUESTION 362

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 367

Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the U.S. Federal Government information security standards?

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

- A. SA System and Services Acquisition
- B. CA Certification, Accreditation, and Security Assessments
- C. IR Incident Response
- D. Information systems acquisition, development, and maintenance

Answer: ABC

NEW QUESTION 371

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

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

Answer: B

NEW QUESTION 376

Henry is the project manager of the QBG Project for his company. This project has a budget of \$4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work.

What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?

- A. Cost change control system
- B. Scope change control system

- C. Integrated change control
- D. Configuration management system

Answer: D

NEW QUESTION 379

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 384

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 388

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 391

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 392

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 396

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 398

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

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

Answer: AD

NEW QUESTION 401

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 404

Which of the following statements about the authentication concept of information security management is true?

- A. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual.
- B. It ensures that modifications are not made to data by unauthorized personnel or processes .
- C. It establishes the users' identity and ensures that the users are who they say they are.
- D. It ensures the reliable and timely access to resources.

Answer: C

NEW QUESTION 407

What are the responsibilities of a system owner?

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

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

Answer: ABC

NEW QUESTION 409

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 412

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

Each correct answer represents a complete solution. Choose two.

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

Answer: AB

NEW QUESTION 415

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 419

You are the project manager of QSL project for your organization. You are working you??re 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 422

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

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

Answer: ACD

NEW QUESTION 427

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

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

Answer: C

NEW QUESTION 430

There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

- A. Exploit
- B. Share
- C. Enhance
- D. Acceptance

Answer: D

NEW QUESTION 432

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 433

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 434

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 436

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 438

What does RTM stand for?

- A. Resource Testing Method
- B. Replaced Traceability Matrix
- C. Requirements Traceability Matrix
- D. Resource Tracking Matrix

Answer: C

NEW QUESTION 441

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 446

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 451

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 452

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 455

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 459

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

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

Answer: C

NEW QUESTION 461

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 463

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 465

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 470

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 473

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

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

Answer: C

NEW QUESTION 475

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 479

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 483

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

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

Answer: A

NEW QUESTION 486

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 490

Which of the following NIST documents defines impact?

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

Answer: D

NEW QUESTION 492

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 495

Which of the following individuals makes the final accreditation decision?

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

Answer: A

NEW QUESTION 498

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

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

Answer: D

NEW QUESTION 502

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 507

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 512

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 515

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 517

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

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

Answer: A

NEW QUESTION 522

Harry is a project manager of a software development project. In the early stages of planning, he and the stakeholders operated with the belief that the software they were developing would work with their organization's current computer operating system. Now that the project team has started developing the software it has become apparent that the software will not work with nearly half of the organization's computer operating systems. The incorrect belief Harry had in the software compatibility is an example of what in project management?

- A. Assumption
- B. Issue
- C. Risk
- D. Constraint

Answer: A

NEW QUESTION 524

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 526

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 530

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 534

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 537

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

Answer: C

NEW QUESTION 542

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 544

.....

Relate Links

100% Pass Your CAP Exam with ExamBible Prep Materials

<https://www.exambible.com/CAP-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>