ISC2

Exam Questions CAP

ISC2 CAP Certified Authorization Professional

NEW QUESTION 1
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 2
Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

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

Answer: B

NEW QUESTION 3
Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

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

Answer: D

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

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

Answer: C

NEW QUESTION 6
Which of the following is a subset discipline of Corporate Governance focused on information security systems and their performance and risk management?

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

Answer: B

NEW QUESTION 7
Your project has several risks that may cause serious financial impact should they happen. You have studied the risk events and made some potential risk responses for the risk events but management wants you to do more. They'd like for you to create some type of a chart that identified the risk probability and impact with a financial amount for each risk event. What is the likely outcome of creating this type of chart?

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

Answer: D

NEW QUESTION 8
Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?

A. Authorizing Official
B. Chief Risk Officer (CRO)
C. Chief Information Officer (CIO)
D. Information system owner

Answer: D

NEW QUESTION 9
You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

A. Quantitative risk analysis
B. Qualitative risk analysis
C. Requested changes
D. Risk audits

Answer: C

NEW QUESTION 10
The phase 3 of the Risk Management Framework (RMF) process is known as mitigation planning.
Which of the following processes take place in phase 3?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 10
Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. What are the different categories of risk?
Each correct answer represents a complete solution. Choose all that apply.

A. System interaction
B. Human interaction
C. Equipment malfunction
D. Inside and outside attacks
E. Social status
F. Physical damage

Answer: BCDEF

NEW QUESTION 13
James work as an IT systems personnel in SoftTech Inc. He performs the following tasks: Runs regular backups and routine tests of the validity of the backup data.
Performs data restoration from the backups whenever required.
Maintains the retained records in accordance with the established information classification policy.
What is the role played by James in the organization?

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

Answer: D

NEW QUESTION 16
Which of the following is an entry in an object's discretionary access control list (DACL) that grants permissions to a user or group?

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

Answer: A

NEW QUESTION 17
You are the project manager for your organization. You have identified a risk event you??re your organization could manage internally or externally. If you manage the event internally it will cost your project $578,000 and an additional $12,000 per month the solution is in use. A vendor can manage the risk event for you. The vendor will charge $550,000 and $14,500 per month that the solution is in use. How many months will you need to use the solution to pay for the internal solution in comparison to the vendor's solution?

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

Answer: B

NEW QUESTION 21
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 23
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 28
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 30
Which of the following assessment methodologies defines a six-step technical security evaluation?

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

Answer: D

NEW QUESTION 31
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 34
Gary is the project manager for his project. He and the project team have completed the qualitative risk analysis process and are about to enter the quantitative risk analysis process when
Mary, the project sponsor, wants to know what quantitative risk analysis will review. Which of the following statements best defines what quantitative risk analysis will review?

A. The quantitative risk analysis seeks to determine the true cost of each identified risk event and the probability of each risk event to determine the risk exposure.
B. The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.
C. The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.

D. The quantitative risk analysis process will analyze the effect of risk events that may substantially impact the project's competing demands.

Answer: D

NEW QUESTION 39
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 43
Which of the following RMF phases is known as risk analysis?

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

Answer: A

NEW QUESTION 46
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 50
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 53
Which of the following are included in Physical Controls?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABEF

NEW QUESTION 55
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 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 thecurrent project.
D. You will use organizational process assets for information from prior similar projects.

Answer: C

NEW QUESTION 60
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 63
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 68
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 71
The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABCD

NEW QUESTION 75
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 77
To help review or design security controls, they can be classified by several criteria. One of these criteria is based on nature. According to this criteria, which of the following controls consists of incident response processes, management oversight, security awareness, and training?

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

Answer: C

NEW QUESTION 80
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 81
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 86
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 87
Which of the following concepts represent the three fundamental principles of information security?
Each correct answer represents a complete solution. Choose three.

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

Answer: BCD

NEW QUESTION 88
Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

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

Answer: B

NEW QUESTION 90
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 95
During qualitative risk analysis you want to define the risk urgency assessment. All of the following are indicators of risk priority except for which one?

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

Answer: C

NEW QUESTION 97
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 101
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 104
Courtney is the project manager for her organization. She is working with the project team to complete the qualitative risk analysis for her project. During the analysis Courtney encourages the project team to begin the grouping of identified risks by common causes. What is the primary advantage to group risks by common causes during qualitative risk analysis?

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

Answer: A

NEW QUESTION 109
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 directlyaffects them

Answer: B

NEW QUESTION 111
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 116
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 120
There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

A. Acceptance
B. Mitigation

C. Sharing
D. Transference

Answer: A

NEW QUESTION 123
What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

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

Answer: C

NEW QUESTION 125
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 130
Which of the following approaches can be used to build a security program?
Each correct answer represents a complete solution. Choose all that apply.

A. Bottom-Up Approach
B. Right-Up Approach
C. Top-Down Approach
D. Left-Up Approach

Answer: AC

NEW QUESTION 134
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 138
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 143
A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy?
Each correct answer represents a part of the solution. Choose all that apply.

A. Who is expected to exploit the vulnerability?
B. What is being secured?
C. Where is the vulnerability, threat, or risk?
D. Who is expected to comply with the policy?

Answer: BCD

NEW QUESTION 148
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 151
Which of the following objectives are defined by integrity in the C.I.A triad of information security systems?
Each correct answer represents a part of the solution. Choose three.

A. It preserves the internal and external consistency of information.
B. It prevents the unauthorized or unintentional modification of information by the authorized users.
C. It prevents the intentional or unintentional unauthorized disclosure of a message's contents .
D. It prevents the modification of information by the unauthorized users.

Answer: ABD

NEW QUESTION 156
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 160
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. SSAA
B. FIPS
C. FITSAF
D. TCSEC

Answer: A

NEW QUESTION 165
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 168
You are the project manager of the GHY project for your organization. You are working with your project team to begin identifying risks for the project. As part of your preparation for identifying the risks within the project you will need eleven inputs for the process. Which one of the following is NOT an input to the risk identification process?

A. Cost management plan
B. Quality management plan
C. Procurement management plan
D. Stakeholder register

Answer: C

NEW QUESTION 170
Mary is the project manager of the HGH Project for her company. She and her project team have agreed that if the vendor is late by more than ten days they will cancel the order and hire the NBG Company to fulfill the order. The NBG Company can guarantee orders within three days, but the costs of their products are significantly more expensive than the current vendor. What type of a response strategy is this?

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

Answer: C

NEW QUESTION 174
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 177
You work as a project manager for BlueWell Inc. Your project is running late and you must respond to the risk. Which risk response can you choose that will also cause you to update the human resource management plan?

A. Teamingagreements
B. Crashing the project
C. Transference
D. Fast tracking the project

Answer: B

NEW QUESTION 182
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 185
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 187
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 188
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 191
Which of the following individuals informs all C&A participants about life cycle actions, security requirements, and documented user needs?

A. IS program manager

B. Certification Agent
C. User representative
D. DAA

Answer: A

NEW QUESTION 192
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 197
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 198
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 203
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 208
Which of the following is NOT a responsibility of a data owner?

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

Answer: A

NEW QUESTION 212
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 216

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 218
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 220
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 224
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 229
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 231
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 235
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 236
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 238
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 242
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 246
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 249
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 251
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 256
Which of the following components ensures that risks are examined for all new proposed change requests in the change control system?

A. Risk monitoring and control
B. Scope change control
C. Configuration management
D. Integrated change control

Answer: D

NEW QUESTION 258
Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could

affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

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

Answer: A

NEW QUESTION 259
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 261
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 263
Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

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

Answer: B

NEW QUESTION 266
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 271
The only output of the perform qualitative risk analysis are risk register updates. When the project manager updates the risk register he will need to include several pieces of information including all of the following except for which one?

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

Answer: B

NEW QUESTION 275
Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?

A. At every status meeting the project team project risk management is an agenda item.
B. Project risk management happens at every milestone.

C. Project risk management has been concluded with the project planning.
D. Project risk management is scheduled for every monthin the 18-month project.

Answer: A

NEW QUESTION 278
Rob is the project manager of the IDLK Project for his company. This project has a budget of $5,600,000 and is expected to last 18 months. Rob has learned that a new law may affect how the project is allowed to proceed - even though the organization has already invested over $750,000 in the project. What risk response is the most appropriate for this instance?

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

Answer: D

NEW QUESTION 283
You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?

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

Answer: A

NEW QUESTION 285
Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process?

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

Answer: D

NEW QUESTION 288
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 291
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 296
A high-profile, high-priority project within your organization is being created. Management wants you to pay special attention to the project risks and do all that you can to ensure that all of the risks are identified early in the project. Management has to ensure that this project succeeds.
Management's risk aversion in this project is associated with what term?

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

Answer: A

NEW QUESTION 300
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 304
Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?

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

Answer: C

NEW QUESTION 305
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 308
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

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

Answer: A

NEW QUESTION 312
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 314
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 315
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 319

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 321
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. The project documents will help the project manager, or Joan, to identify what risk identification approach is best to pursue.
B. Plans that have loose definitions of terms and disconnected approaches will reveal risks.
C. Poorly written requirements will reveal inconsistencies in the project plans and documents.
D. Lack of consistency between the plans and the project requirements and assumptions can be the indicators of risk in the project.

Answer: D

NEW QUESTION 323
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 324
Which of the following are the objectives of the security certification documentation task?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABCD

NEW QUESTION 327
You are the project manager for your organization. You are working with your project team to complete the qualitative risk analysis process. The first tool and technique you are using requires that you assess the probability and what other characteristic of each identified risk in the project?

A. Risk owner
B. Risk category
C. Impact
D. Cost

Answer: C

NEW QUESTION 330
You work as a project manager for BlueWell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decided, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project which of the following are likely to increase?

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

Answer: C

NEW QUESTION 332
Information Security management is a process of defining the security controls in order to protect information assets. What are the security management responsibilities?
Each correct answer represents a complete solution. Choose all that apply.

A. Evaluating business objectives, security risks, user productivity, and functionality requirem ents
B. Determining actual goals that are expected to be accomplished from a security program
C. Defining steps to ensure that all the responsibilities are accounted for and properly address ed
D. Determining objectives, scope, policies, priorities, standards, and strategies

Answer: ABCD

NEW QUESTION 334
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 337
The National Information Assurace 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 340
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 345
There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

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

Answer: C

NEW QUESTION 347
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 350
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 355
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 359
You work as a project manager for TechSoft Inc. You are working with the project stakeholders onthe qualitative risk analysis process in your project. You have used all the tools to the qualitative risk analysis process in your project. Which of the following techniques is NOT used as a tool in qualitative risk analysis process?

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

Answer: A

NEW QUESTION 363
Tracy is the project manager of the NLT Project for her company. The NLT Project is scheduled to last 14 months and has a budget at completion of $4,555,000. Tracy's organization will receive a bonus of $80,000 per day that the project is completed early up to $800,000. Tracy realizes that there are several opportunities within the project to save on time by crashing the project work.
Crashing the project is what type of risk response?

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

Answer: C

NEW QUESTION 364
Diana is the project manager of the QPS project for her company. In this project Diana and the project team have identified a pure risk. Diana and the project team decided, along with the key stakeholders, to remove the pure risk from the project by changing the project plan altogether.
What is a pure risk?

A. It is a risk event that only has a negative side, such as loss of life or limb.
B. It is a risk event that cannot be avoided because of the order of the work.
C. It is a risk event that is created by a risk response.
D. It is a risk event that is generated due to errors or omission in the project work.

Answer: A

NEW QUESTION 368
You work as a project manager for BlueWell Inc. You are about to complete the quantitative risk analysis process for your project. You can use three available tools and techniques to complete this process. Which one of the following is NOT a tool or technique that is appropriate for the quantitative risk analysis process?

A. Quantitative risk analysis andmodeling techniques
B. Data gathering and representation techniques
C. Expert judgment
D. Organizational process assets

Answer: D

NEW QUESTION 369
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 370
David is the project manager of HGF project for his company. David, the project team, and several key stakeholders have completed risk identification and are ready to move into qualitative risk analysis. Tracy, a project team member, does not understand why they need to complete qualitative risk analysis. Which one of the following is the best explanation for completing qualitative risk analysis?

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

D. All risks must pass through quantitative risk analysis before qualitative risk analysis.

Answer: A

NEW QUESTION 373
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 374
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 379
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 384
Which of the following individuals makes the final accreditation decision?

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

Answer: B

NEW QUESTION 385
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 388
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. Issue
B. Risk
C. Constraint
D. Assumption

Answer: D

NEW QUESTION 389
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 391
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 392
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 397
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 401
Jenny is the project manager for the NBT projects. She is working with the project team and several subject matter experts to perform the quantitative risk analysis process. During this process she and the project team uncover several risks events that were not previously identified.
What should Jenny do with these risk events?

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

Answer: D

NEW QUESTION 406
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 411
You are the project manager of the BlueStar 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 qualitative risk analysis process. What will you need as inputs for the qualitative risk analysis of the project in this scenario?

A. You will need the risk register, risk management plan, project scope statement, 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, permission from the functional manager, and any relevant organizational process assets.
D. Qualitative risk analysis does not happen through the project manager in a functional struc ture.

Answer: A

NEW QUESTION 412
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 implement ation
D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

Answer: BCD

NEW QUESTION 414
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 416
You are the project manager of the NHQ project for your company. Management has told you that you must implement an agreed upon contingency response if the Cost Performance Index in your project is less than 0.90. Consider that your project has a budget at completion of $250,000 and is 60 percent complete. You are scheduled to be however, 75 percent complete, and you have spent $165,000 to date. What is the Cost Performance Index for this project to determine if the contingency response should happen?

A. 0.88
B. 0.80
C. -$37,500
D. 0.91

Answer: D

NEW QUESTION 420
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 422
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 423
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 425
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 428
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 430
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 434
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 437
You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?

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

Answer: D

NEW QUESTION 441
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 443
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 444

Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

A. The custodian implements the information classification scheme after the initial assignment by the operations manager.
B. The datacustodian implements the information classification scheme after the initial assignment by the data owner.
C. The data owner implements the information classification scheme after the initial assignment by the custodian.
D. The custodian makes the initialinformation classification assignments, and the operations manager implements the scheme.

Answer: B

NEW QUESTION 445
Which of the following NIST C&A documents is the guideline for identifying an information system as a National Security System?

A. NIST SP800-53
B. NIST SP 800-59
C. NIST SP 800-37
D. NIST SP 800-53A

Answer: B

NEW QUESTION 447
Which of the following system security policies is used to address specific issues of concern to the organization?

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

Answer: B

NEW QUESTION 450
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 453
In which of the following DITSCAP phases is the SSAA developed?

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

Answer: C

NEW QUESTION 457
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 458
Which of the following parts of BS 7799 covers risk analysis and management?

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

Answer: B

NEW QUESTION 461
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 462
Which of the following individuals is responsible for the final accreditation decision?

A. Information System Owner
B. Certification Agent
C. User Representative
D. Risk Executive

Answer: A

NEW QUESTION 467
Which of the following processes has the goal to ensure that any change does not lead to reduced or compromised security?

A. Risk management
B. Security management
C. Configuration management
D. Changecontrol management

Answer: D

NEW QUESTION 471
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 475
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 478
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 481
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 485
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 488
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 492
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 497
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 498
Which of the following relations correctly describes total risk?

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

Answer: A

NEW QUESTION 500
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 501
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 503
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 504
Which of the following guidance documents is useful in determining the impact level of a particular threat on agency systems?

A. NIST SP 800-41
B. NIST SP 800-37

C. FIPS 199
D. NIST SP 800-14

Answer: C

NEW QUESTION 507
Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

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

Answer: D

NEW QUESTION 508
In which type of access control do user ID and password system come under?

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

Answer: B

NEW QUESTION 513
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 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 519
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 523
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 526
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 531
During qualitative risk analysis you want to define the risk urgency assessment. All of the following are indicators of risk priority except for which one?

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

Answer: B

NEW QUESTION 535
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 list containing user accounts, groups, and computers that are allowed (or denied) access to the object.
D. It is a unique number that identifies a user, group, and computer account

Answer: C

NEW QUESTION 540
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 542
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 546
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAP Practice Exam Features:

* CAP Questions and Answers Updated Frequently

* CAP Practice Questions Verified by Expert Senior Certified Staff

* CAP Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CAP Practice Test Here