

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

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 3

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 4

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 5

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 6

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP?

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

- A. Validation
- B. Re-Accreditation
- C. Verification
- D. System Definition
- E. Identification
- F. Accreditation

Answer: ABCD

NEW QUESTION 7

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 8

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 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

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

- A. DoDD 8000.1
- B. DoD 7950.1-M
- C. DoD 5200.22-M
- D. DoD 8910.1
- E. DoD 5200.1-R

Answer: B

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 12

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

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

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

Answer: A

NEW QUESTION 16

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 19

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

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

Answer: B

NEW QUESTION 22

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 26

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 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

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. Resource breakdown structure
- C. RACI chart
- D. Roles and responsibility matrix

Answer: B

NEW QUESTION 34

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

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

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

Answer: B

NEW QUESTION 41

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 44

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

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

Answer: C

NEW QUESTION 48

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

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

Answer: D

NEW QUESTION 51

You are the project manager of the NNH Project. In this project you have created a contingency response that the schedule performance index should be less than 0.93. The NNH Project has a budget at completion of \$945,000 and is 45 percent complete though the project should be 49 percent complete. The project has spent \$455,897 to reach the 45 percent complete milestone.

What is the project's schedule performance index?

- A. 1.06
- B. 0.92
- C. -\$37,800
- D. 0.93

Answer: B

NEW QUESTION 56

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

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

Answer: C

NEW QUESTION 57

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 63

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

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

Answer: B

NEW QUESTION 64

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

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

Answer: D

NEW QUESTION 67

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 68

You are the project manager for the NHH project. You are working with your project team to examine the project from four different defined perspectives to increase the breadth of identified risks by including internally generated risks. What risk identification approach are you using in this example?

- A. SWOT analysis
- B. Root cause analysis
- C. Assumptions analysis
- D. Influence diagramming techniques

Answer: A

NEW QUESTION 69

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 71

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 75

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 76

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 81

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 84

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 86

You are the project manager of the GHQ project for your company. You are working with your project team to prepare for the qualitative risk analysis process. Mary, a project team member, does not understand why you need to complete qualitative risks analysis. You explain to Mary that qualitative risks analysis helps you determine which risks need additional analysis. There are also some other benefits that qualitative risks analysis can do for the project. Which one of the following is NOT an accomplishment of the qualitative risk analysis process?

- A. Cost of the risk impact if the risk event occurs
- B. Corresponding impact on project objectives
- C. Time frame for a risk response
- D. Prioritization of identified risk events based on probability and impact

Answer: A

NEW QUESTION 89

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 93

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 97

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 101

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 105

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 107

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

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 111

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 113

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 116

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 117

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 122

You work as the project manager for Bluewell Inc. You are working on NGQQ Project you're your company. You have completed the risk analysis processes for the risk events. You and the project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transference
- D. Risk mitigation

Answer: C

NEW QUESTION 124

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

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

Answer: B

NEW QUESTION 128

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

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

Answer: B

NEW QUESTION 131

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 you're 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 133

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 136

Which of the following is the acronym of RTM?

- A. Resource tracking method
- B. Requirements Traceability Matrix
- C. Resource timing method
- D. Requirements Testing Matrix

Answer: B

NEW QUESTION 141

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 146

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 150

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 153

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

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

Answer: A

NEW QUESTION 155

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 158

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 163

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 164

Which of the following statements is true about residual risks?

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

Answer: C

NEW QUESTION 169

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 174

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 176

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 180

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 181

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

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

Answer: B

NEW QUESTION 183

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

Joan is a project management consultant and she has been hired by a firm to help them identify risk events within the project. Joan would first like to examine the project documents including the plans, assumptions lists, project files, and contracts. What key thing will help Joan to discover risks within the review of the project documents?

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

Answer: A

NEW QUESTION 189

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

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

Answer: D

NEW QUESTION 190

You are the project manager of the NNH Project. In this project you have created a contingency response that the schedule performance index should be less than 0.93. The NNH Project has a budget at completion of \$945,000 and is 45 percent complete though the project should be 49 percent complete. The project has spent \$455,897 to reach the 45 percent complete milestone. What is the project's schedule performance index?

- A. 1.06
- B. 0.93
- C. -\$37,800
- D. 0.92

Answer: D

NEW QUESTION 192

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 197

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 198

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 199

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 204

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 206

Which of the following relations correctly describes residual risk?

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

Answer: D

NEW QUESTION 208

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 211

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 215

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 217

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 219

What approach can a project manager use to improve the project's performance during qualitative risk analysis?

- A. Create a risk breakdown structure and delegate the risk analysis to the appropriate project team members.
- B. Focus on high-priority risks.
- C. Focus on near-term risks first.
- D. Analyze as many risks as possible regardless of who initiated the risk event.

Answer: B

NEW QUESTION 224

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 226

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 227

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 230

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 231

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 235

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 237

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 241

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 246

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 248

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 249

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

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

D. Project risk management is scheduled for every month in the 18-month project.

Answer: A

NEW QUESTION 250

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 252

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

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

Answer: A

NEW QUESTION 256

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 258

FITSAP 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 are tested and reviewed?

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

Answer: C

NEW QUESTION 262

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

- A. Utility function
- B. Risk conscience
- C. Quantitative risk analysis
- D. Risk mitigation

Answer: A

NEW QUESTION 267

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

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

Answer: BCD

NEW QUESTION 269

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 270

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

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

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

Answer: D

NEW QUESTION 273

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 278

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 283

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 286

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 290

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing?

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

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

Answer: BCDEF

NEW QUESTION 293

You are the project manager for TTP project. You are in the Identify Risks process. You have to create the risk register. Which of the following are included in the risk register?

Each correct answer represents a complete solution. Choose two.

- A. List of potential responses
- B. List of identified risks
- C. List of mitigation techniques
- D. List of key stakeholders

Answer: AB

NEW QUESTION 295

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

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

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

Answer: ABDE

NEW QUESTION 300

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 303

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

Answer: ABC

NEW QUESTION 305

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

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

Answer: D

NEW QUESTION 307

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 312

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 316

Gary is the project manager for his organization. He is working with the project stakeholders on the project requirements and how risks may affect their project. One of the stakeholders is confused about what constitutes risks in the project. Which of the following is the most accurate definition of a project risk?

- A. It is an uncertain event that can affect the project costs.
- B. It is an uncertain event or condition within the project execution.
- C. It is an uncertain event that can affect at least one project objective.
- D. It is an unknown event that can affect the project scope.

Answer: C

NEW QUESTION 318

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

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

Answer: A

NEW QUESTION 319

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

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

Answer: B

NEW QUESTION 321

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 325

The Identify Risk process determines the risks that affect the project and document their characteristics. Why should the project team members be involved in the Identify Risk process?

- A. They are the individuals that will have the best responses for identified risks events within the project.
- B. They are the individuals that are most affected by the risk events.
- C. They are the individuals that will need a sense of ownership and responsibility for the risk events.
- D. They are the individuals that will most likely cause and respond to the risk events.

Answer: C

NEW QUESTION 326

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 328

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 333

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 338

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 340

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

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

Answer: D

NEW QUESTION 342

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 344

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 348

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 350

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

"This is the process of numerically analyzing the effect of identified risks on overall project objectives."

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

Answer: B

NEW QUESTION 351

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

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

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

Answer: ABC

NEW QUESTION 352

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 355

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 358

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 structure.

Answer: A

NEW QUESTION 360

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 361

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 362

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 366

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 371

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 372

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 376

Diane is the project manager of the HGF Project. A risk that has been identified and analyzed in the project planning processes is now coming into fruition. What individual should respond to the risk with the preplanned risk response?

- A. Diane
- B. Risk owner

- C. Subject matter expert
- D. Project sponsor

Answer: B

NEW QUESTION 380

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 385

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 388

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 393

You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

- A. Qualitative risk analysis
- B. Seven risk responses
- C. Quantitative risk analysis
- D. A risk probability-impact matrix

Answer: A

NEW QUESTION 394

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 396

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 398

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 403

Which of the following statements about role-based access control (RBAC) model is true?

- A. In this model, the permissions are uniquely assigned to each user account.
- B. In this model, a user can access resources according to his role in the organization.
- C. In this model, the same permission is assigned to each user account.
- D. In this model, the users can access resources according to their seniority.

Answer: B

NEW QUESTION 407

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 410

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 412

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 417

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 422

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 424

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 425

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 429

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 430

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 434

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

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

Answer: D

NEW QUESTION 436

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 437

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 439

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 443

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

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

Answer: B

NEW QUESTION 444

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 449

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 453

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 457

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 459

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

- A. DoD 5200.22-M
- B. DoD 5200.1-R
- C. DoD 8910.1
- D. DoDD 8000.1
- E. DoD 7950.1-M

Answer: E

NEW QUESTION 461

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 463

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 464

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 469

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 472

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 473

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

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

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

Answer: CDE

NEW QUESTION 477

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 481

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 483

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

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

Answer: C

NEW QUESTION 486

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 490

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 491

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 493

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

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

Answer: A

NEW QUESTION 497

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * CAP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CAP Practice Test Here](#)