

## CAP Dumps

### ISC2 CAP Certified Authorization Professional

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



**NEW QUESTION 1**

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

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

**Answer:** C

**NEW QUESTION 2**

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

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

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

**Answer:** ACD

**NEW QUESTION 3**

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 4**

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

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

**Answer:** A

**NEW QUESTION 5**

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 6**

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 7**

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 8

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production?

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

- A. NIST
- B. FIPS
- C. FISMA
- D. Office of Management and Budget (OMB)

**Answer:** CD

#### NEW QUESTION 9

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

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

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

**Answer:** BCD

#### NEW QUESTION 10

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD?

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

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

**Answer:** ABC

#### NEW QUESTION 10

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 11

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 13

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 17

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 21

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 23

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 24

Neil works as a project manager for SoftTech Inc. He is working with Tom, the COO of his company, on several risks within the project. Tom understands that through qualitative analysis Neil has identified many risks in the project. Tom's concern, however, is that the priority list of these risk events are sorted in "high-risk," "moderate-risk," and "low-risk" as conditions apply within the project. Tom wants to know that is there any other objective on which Neil can make the priority list for project risks. What will be Neil's reply to Tom?

- A. Risk may be listed by the responses in the near-term
- B. Risks may be listed by categories
- C. Risks may be listed by the additional analysis and response
- D. Risks may be listed by priority separately for schedule, cost, and performance

**Answer:** D

#### NEW QUESTION 26

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

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

**Answer:** B

#### NEW QUESTION 31

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 32

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 37

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 39

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 41

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 46

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

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

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

**Answer:** ABDE

#### NEW QUESTION 48

Risks with low ratings of probability and impact are included on a \_\_\_\_ for future monitoring.

- A. Watchlist
- B. Risk alarm
- C. Observation list
- D. Risk register

**Answer:** A

#### NEW QUESTION 49

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 51

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 55

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

What is the project's schedule performance index?

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

**Answer:** B

#### NEW QUESTION 56

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

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

**Answer:** B

#### NEW QUESTION 57

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 59

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 60

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 64

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 66



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

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 75

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 76

Which of the following are included in Administrative Controls?

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

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

**Answer: ABDE**

#### NEW QUESTION 79

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 84

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 88

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

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

**Answer:** ABCE

#### NEW QUESTION 90

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 95

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 100

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 105

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 107

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

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



**Answer:** D

**NEW QUESTION 108**

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

- A. Circumstantial
- B. Incontrovertible
- C. Direct
- D. Corroborating

**Answer:** A

**NEW QUESTION 113**

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

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

**Answer:** D

**NEW QUESTION 117**

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 118**

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 121**

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

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

**Answer:** B

**NEW QUESTION 125**

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 129**

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 132**

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 136**

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 140**

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 142**

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 147**

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 150**

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 155**

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 159

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 161

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 162

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 166

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

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

**Answer:** ABC

#### NEW QUESTION 168

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

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

**Answer:** B

#### NEW QUESTION 169

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 170**

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

**Answer:** ABDE

**NEW QUESTION 174**

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 177**

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

Each correct answer represents a complete solution. Choose two.

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

**Answer:** AD

**NEW QUESTION 181**

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 182**

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 184**

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 Response Plan

**Answer:** A

**NEW QUESTION 188**

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 189

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 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 194

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

What should Walter also update in this scenario considering the risk event?

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

**Answer:** B

#### NEW QUESTION 195

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

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

**Answer:** D

#### NEW QUESTION 198

Which of the following phases begins with a review of the SSAA in the DITSCAP accreditation?

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

**Answer:** C

#### NEW QUESTION 203

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 205**

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

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

**Answer:** B

**NEW QUESTION 209**

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 213**

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 217**

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 220**

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

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

**Answer:** C

**NEW QUESTION 221**

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

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

**Answer:** A

**NEW QUESTION 223**

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

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

**Answer:** D

**NEW QUESTION 224**

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 227

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

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

**Answer:** A

#### NEW QUESTION 230

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 235

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 240

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 241

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

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

**Answer:** B

#### NEW QUESTION 242

Which of the following 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 243

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

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

**Answer:** A

#### NEW QUESTION 246

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 248

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 252

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 253

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 256

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 260

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 265

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 270**

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 275**

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 280**

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 284**

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 287**

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 are tested and reviewed?

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

**Answer:** C

#### **NEW QUESTION 289**

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 294**

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 297**

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 301**

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 305**

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 310**

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 312**

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

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

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

**Answer:** C

**NEW QUESTION 316**

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 320**

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 321**

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 325**

What NIACAP certification levels are recommended by the certifier?  
Each correct answer represents a complete solution. Choose all that apply.

- A. Minimum Analysis
- B. Basic System Review
- C. Detailed Analysis
- D. Maximum Analysis
- E. Comprehensive Analysis
- F. Basic Security Review

**Answer:** ACEF

**NEW QUESTION 326**

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 328**

You are the project manager of the HJK project for your organization. You and the project team have created risk responses for many of the risk events in the project. A teaming agreement is an example of what risk response?

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

**Answer:** C

**NEW QUESTION 331**

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 334**

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

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

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

**Answer:** BCDE

#### NEW QUESTION 337

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 338

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 340

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 342

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 343

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

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

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

**Answer:** BCD

#### NEW QUESTION 346

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

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

**Answer:** A



**NEW QUESTION 349**

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 354**

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 357**

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

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

**Answer: B**

**NEW QUESTION 362**

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 366**

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

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

**Answer: D**

**NEW QUESTION 370**

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 375**

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 376

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 378

Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

- A. Protect society, the commonwealth, and the infrastructure.
- B. Act honorably, honestly, justly, responsibly, and legally.
- C. Provide diligent and competent service to principals.
- D. Give guidance for resolving good versus good and bad versus bad dilemmas.

**Answer:** ABC

#### NEW QUESTION 379

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

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

**Answer:** D

#### NEW QUESTION 384

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

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

**Answer:** A

#### NEW QUESTION 389

Which of the following individuals makes the final accreditation decision?

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

**Answer:** B

#### NEW QUESTION 392

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 396

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199.

What levels of potential impact are defined by FIPS 199?

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

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

**Answer:** ABC

#### NEW QUESTION 400

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 403

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 408

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 413

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

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 419

You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

- A. It is a risk that remains because no risk response is taken.
- B. It is a risk that remains after planned risk responses are taken.
- C. It is a risk that can not be addressed by a risk response.
- D. It is a risk that will remain no matter what type of risk response is offered.

**Answer:** B

**NEW QUESTION 421**

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 423**

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 427**

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

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

**Answer: A**

**NEW QUESTION 429**

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 432**

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 437**

NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews?

- A. Substantial
- B. Significant
- C. Abbreviated
- D. Comprehensive

**Answer: C**

**NEW QUESTION 438**

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, remote access controls, operating system configurations, and so on.
- D. Ensures that the necessary security controls are in place.

**Answer:** ABC

**NEW QUESTION 442**

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 445**

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

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

**Answer:** AB

**NEW QUESTION 447**

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 449**

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

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

**Answer:** B

**NEW QUESTION 451**

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 454**

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

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

**Answer:** D

**NEW QUESTION 457**

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 459**

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 464**

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 469**

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 474**

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 476**

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 481**

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 483**

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 484**



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 489**

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

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

**Answer:** A

**NEW QUESTION 493**

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 495**

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 498**

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 501**

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 505**

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 510**

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 512**

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 513**

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 514**

For which of the following reporting requirements are continuous monitoring documentation reports used?

- A. FISMA
- B. NIST
- C. HIPAA
- D. FBI

**Answer:** A

**NEW QUESTION 516**

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

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

**Answer:** B

**NEW QUESTION 517**

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 518**

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 522**

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 525**

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 530**

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

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

**Answer:** A

**NEW QUESTION 533**

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 536**

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 538**

In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199.

What levels of potential impact are defined by FIPS 199?

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

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

**Answer:** ACD

**NEW QUESTION 541**

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 542**

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 545**

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 549**

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 552**

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 554**

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 559**

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

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

\* One year free update

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

\* Trusted by Millions

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

\* Shop Securely

All transactions are protected by VeriSign!

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

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