



ISC2

Exam Questions CAP

ISC2 CAP Certified Authorization Professional

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

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

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

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

Answer: ACD

NEW QUESTION 2

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

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

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

Answer: ACE

NEW QUESTION 3

Which of the following assessment methodologies defines a six-step technical security evaluation?

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

Answer: B

NEW QUESTION 4

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 5

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 6

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 7

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 8

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 9

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 10

What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

- A. Develop DIACAP strategy.
- B. Assign IA controls.
- C. Assemble DIACAP team.
- D. Initiate IA implementation plan.
- E. Register system with DoD Component IA Program.
- F. Conduct validation activity.

Answer: ABCDE

NEW QUESTION 10

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

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

Answer: BCDEF

NEW QUESTION 12

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 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

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 22

In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

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

Answer: B

NEW QUESTION 24

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

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

Answer: D

NEW QUESTION 26

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 28

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

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

Answer: C

NEW QUESTION 29

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 34

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 39

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 42

Jenny is the project manager of the NHJ Project for her company. She has identified several positive risk events within the project and she thinks these events can save the project time and money. You, a new team member wants to know that how many risk responses are available for a positive risk event. What will Jenny reply to you?

- A. Four
- B. Seven
- C. Acceptance is the only risk response for positive risk events.
- D. Three

Answer: A

NEW QUESTION 45

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 46

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

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

Answer: ABEF

NEW QUESTION 48

Which of the following NIST Special Publication documents provides a guideline on network security testing?

- A. NIST SP 800-60
- B. NIST SP 800-53A
- C. NIST SP 800-37
- D. NIST SP 800-42
- E. NIST SP 800-59
- F. NIST SP 800-53

Answer: D

NEW QUESTION 49

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 53

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 56

You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

- A. Sharing
- B. Avoidance
- C. Transference
- D. Exploiting

Answer: C

NEW QUESTION 60

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

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

Answer: A

NEW QUESTION 65

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 69

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 72

What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

- A. Configuration Management System
- B. Project Management InformationSystem
- C. Scope Verification
- D. Integrated Change Control

Answer: A

NEW QUESTION 76

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 78

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 81

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

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

Answer: B

NEW QUESTION 85

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 89

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

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

Answer: D

NEW QUESTION 90

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 93

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

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

Answer: A

NEW QUESTION 97

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 101

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 102

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 103

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 105

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 110

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 113

In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

- A. Full operational test

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

Answer: B

NEW QUESTION 118

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

Answer: B

NEW QUESTION 121

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 126

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

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

Answer: C

NEW QUESTION 129

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 NGB Company to fulfill the order. The NGB 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 134

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 138

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 141

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 143

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

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

Answer: C

NEW QUESTION 146

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 149

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

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

Answer: A

NEW QUESTION 153

Which of the following individuals informs all C&A participants about life cycle actions, security requirements, and documented user needs?

- A. IS program manager
- B. Certification Agent
- C. User representative
- D. DAA

Answer: A

NEW QUESTION 155

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 157

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

- A. 1.06
- B. 0.93

- C. -\$37,800
- D. 0.92

Answer: D

NEW QUESTION 161

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

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

Answer: A

NEW QUESTION 162

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 163

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 166

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 170

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 172

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

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

Answer: B

NEW QUESTION 173

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 175

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 178

Which of the following NIST documents defines impact?

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

Answer: C

NEW QUESTION 180

What is the objective of the Security Accreditation Decision task?

- A. To determine whether the agency-level risk is acceptable or not.
- B. To make an accreditation decision
- C. To accredit the information system
- D. To approve revisions of NIACAP

Answer: A

NEW QUESTION 182

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 185

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

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

Answer: C

NEW QUESTION 187

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 192

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 197

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 202

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 204

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 208

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 212

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 215

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 220

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 225

You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks.

Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

- A. A qualitative risk analysis requires fast and simple data to complete the analysis.
- B. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.
- C. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.
- D. A qualitative risk analysis encourages biased data to reveal risk tolerances.

Answer: B

NEW QUESTION 226

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 228

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

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

Answer: C

NEW QUESTION 230

In which of the following DIACAP phases is residual risk analyzed?

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

Answer: B

NEW QUESTION 232

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 237

Which of the following statements are true about security risks?

Each correct answer represents a complete solution. Choose three.

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

Answer: BCD

NEW QUESTION 240

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 242

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 244

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 245

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 249

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 250

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 251

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 254

Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event?

- A. Corrective action
- B. Technical performance measurement
- C. Risk audit
- D. Earned value management

Answer: A

NEW QUESTION 258

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 259

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

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

Answer: A

NEW QUESTION 260

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 263

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 264

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 268

Information Security management is a process of defining the security controls in order to protect information assets. What are the security management responsibilities?

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

- A. Evaluating business objectives, security risks, user productivity, and functionality requirements
- B. Determining actual goals that are expected to be accomplished from a security program

- C. Defining steps to ensure that all the responsibilities are accounted for and properly address ed
- D. Determining objectives, scope, policies, priorities, standards, and strategies

Answer: ABCD

NEW QUESTION 271

Which of the following are included in Technical Controls?

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

- A. Implementing and maintaining access control mechanisms
- B. Password and resource management
- C. Configuration of the infrastructure
- D. Identification and authentication methods
- E. Conducting security-awareness training
- F. Security devices

Answer: ABCDF

NEW QUESTION 272

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 274

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 278

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 281

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 286

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 287

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 289

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 291

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

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

Answer: A

NEW QUESTION 295

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

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

Answer: D

NEW QUESTION 297

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 301

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 303

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 308

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 309

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 314

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 317

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 320

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 322

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 325

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 329

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 330

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 331

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

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

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

Answer: ABC

NEW QUESTION 332

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 334

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 337

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 341

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 343

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 345

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 350

You are the project manager for a construction project. The project involves casting of a column in a very narrow space. Because of lack of space, casting it is highly dangerous. High technical skill will be required for casting that column. You decide to hire a local expert team for casting that column. Which of the following types of risk response are you following?

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

Answer: C

NEW QUESTION 351

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 354

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 359

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 362

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 365

Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

- A. DITSCAP
- B. NIACAP
- C. NSA-IAM
- D. ASSET

Answer: B

NEW QUESTION 370

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 371

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 372

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

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

Answer: A

NEW QUESTION 375

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 379

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 381

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

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

Answer: C

NEW QUESTION 386

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

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

Answer: C

NEW QUESTION 389

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 391

Which of the following C&A professionals plays the role of an advisor?

- A. Information System Security Engineer (ISSE)
- B. Chief Information Officer (CIO)
- C. Authorizing Official
- D. Information Owner

Answer: A

NEW QUESTION 393

Which of the following individuals is responsible for the final accreditation decision?

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

Answer: C

NEW QUESTION 398

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

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

Answer: B

NEW QUESTION 399

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 401

Which of the following guidance documents is useful in determining the impact level of a particular threat on agency systems?

- A. NIST SP 800-41
- B. NIST SP 800-37
- C. FIPS 199
- D. NIST SP 800-14

Answer: C

NEW QUESTION 404

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

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

Answer: D

NEW QUESTION 408

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 413

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 415

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 416

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

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

Answer: A

NEW QUESTION 419

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 421

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

- A. Symptoms

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

Answer: B

NEW QUESTION 426

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 431

.....

Relate Links

100% Pass Your CAP Exam with ExamBible Prep Materials

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

Contact us

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

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