



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

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 3

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

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

Answer: D

NEW QUESTION 4

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 5

Certification and Accreditation (C&A or CnA) is a process for implementing information security.

Which of the following is the correct order of C&A phases in a DITSCAP assessment?

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

Answer: D

NEW QUESTION 6

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 7

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 8

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

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

Answer: C

NEW QUESTION 9

Where can a project manager find risk-rating rules?

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

Answer: B

NEW QUESTION 10

There are five inputs to the quantitative risk analysis process. Which one of the following is NOT an input to the perform quantitative risk analysis process?

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

Answer: D

NEW QUESTION 10

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 13

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 17

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 19

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 21

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

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 36

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 40

A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

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

Answer: D

NEW QUESTION 42

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 44

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

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

Answer: B

NEW QUESTION 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 50

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 53

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

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

Answer: D

NEW QUESTION 56

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 59

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 61

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 63

You are the project manager of the GHG project. You are preparing for the quantitative risk analysis process. You are using organizational process assets to help you complete the quantitative risk analysis process. Which one of the following is NOT a valid reason to utilize organizational process assets as a part of the quantitative risk analysis process?

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

Answer: C

NEW QUESTION 66

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 modification of information by the unauthorized users.
- D. It prevents the intentional or unintentional unauthorized disclosure of a message's contents .

Answer: ABC

NEW QUESTION 69

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 70

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 73

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

- A. Cost of the risk impact if the risk event occurs
- B. Corresponding impact on project objectives

- C. Time frame for a risk response
- D. Prioritization of identified risk events based on probability and impact

Answer: A

NEW QUESTION 77

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 80

You work as a project manager for BlueWell Inc. Management has asked you to work with the key project stakeholder to analyze the risk events you have identified in the project. They would like you to analyze the project risks with a goal of improving the project's performance as a whole.

What approach can you use to achieve the goal of improving the project's performance through risk analysis with your project stakeholders?

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

Answer: B

NEW QUESTION 82

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 84

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

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

Answer: A

NEW QUESTION 87

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

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

Answer: B

NEW QUESTION 92

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 97

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

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

Answer: A

NEW QUESTION 98

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 100

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 105

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 109

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 110

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 113

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 116

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 118

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 121

Which of the following documents were developed by NIST for conducting Certification & Accreditation (C&A)?

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

- A. NIST Special Publication 800-53A
- B. NIST Special Publication 800-37A
- C. NIST Special Publication 800-59
- D. NIST Special Publication 800-53
- E. NIST Special Publication 800-37
- F. NIST Special Publication 800-60

Answer: ACDEF

NEW QUESTION 125

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 129

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 132

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 135

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 140

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 144

Which of the following methods of authentication uses finger prints to identify users?

- A. PKI
- B. Mutual authentication
- C. Biometrics
- D. Kerberos

Answer: C

NEW QUESTION 145

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 150

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 154

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 156

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 159

Which of the following documents is used to provide a standard approach to the assessment of NIST SP 800-53 security controls?

- A. NIST SP 800-37
- B. NIST SP 800-41
- C. NIST SP 800-53A
- D. NIST SP 800-66

Answer: C

NEW QUESTION 161

You are the project manager for your organization. You are working with your key stakeholders in the qualitative risk analysis process. You understand that there is certain bias towards the risk events in the project that you need to address, manage, and ideally reduce. What solution does the PMBOK recommend to reduce the influence of bias during qualitative risk analysis?

- A. Establish the definitions of the levels of probability and impact
- B. Isolate the stakeholders by project phases to determine their risk bias
- C. Involve all stakeholders to vote on the probability and impact of the risk events
- D. Provide iterations of risk analysis for true reflection of a risk probability and impact

Answer: A

NEW QUESTION 164

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

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

- A. Human resources security
- B. Organization of information security
- C. Risk assessment and treatment
- D. AU audit and accountability

Answer: ABC

NEW QUESTION 167

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 171

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

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

Answer: B

NEW QUESTION 174

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 175

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 177

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 178

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 183

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 187

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 190

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 191

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

- A. At every status meeting the project team project risk management is an agenda item.
- B. Project risk management happens at every milestone.
- C. Project risk management has been concluded with the project planning.
- D. Project risk management is scheduled for every month in the 18-month project.

Answer: A

NEW QUESTION 194

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 196

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 200

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 205

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 208

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 209

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 211

You are the project manager of the NNQ Project for your company and are working you??re your project team to define contingency plans for the risks within your project. Mary, one of your project team members, asks what a contingency plan is. Which of the following statements best defines what a contingency response is?

- A. Some responses are designed for use only if certain events occur.
- B. Some responses have a cost and a time factor to consider for each risk event.
- C. Some responses must counteract pending risk events.
- D. Quantified risks should always have contingency responses.

Answer: A

NEW QUESTION 214

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 219

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 224

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 226

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

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

Answer: ABCD

NEW QUESTION 228

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 addressed
- D. Determining objectives, scope, policies, priorities, standards, and strategies

Answer: ABCD

NEW QUESTION 231

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 232

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 236

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 240

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 241

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 242

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 244

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 247

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 252

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

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

Answer: E

NEW QUESTION 253

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 257

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies?

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

- A. Systematic
- B. Informative
- C. Regulatory
- D. Advisory

Answer: BCD

NEW QUESTION 261

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 263

Jenny is the project manager for the NBT projects. She is working with the project team and several subject matter experts to perform the quantitative risk analysis process. During this process she and the project team uncover several risks events that were not previously identified.

What should Jenny do with these risk events?

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

Answer: D

NEW QUESTION 264

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

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

Answer: B

NEW QUESTION 265

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

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

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

Answer: D

NEW QUESTION 268

Which of the following are the goals of risk management?

Each correct answer represents a complete solution. Choose three.

- A. Finding an economic balance between the impact of the risk and the cost of the countermeasures
- B. Identifying the risk
- C. Assessing the impact of potential threats
- D. Identifying the accused

Answer: ABC

NEW QUESTION 272

Elizabeth is a project manager for her organization and she finds risk management to be very difficult for her to manage. She asks you, a lead project manager, at what stage in the project will risk management become easier. What answer best resolves the difficulty of risk management practices and the effort required?

- A. Risk management only becomes easier the more often it is practiced.
- B. Risk management is an iterative process and never becomes easier.
- C. Risk management only becomes easier when the project moves into project execution.
- D. Risk management only becomes easier when the project is closed.

Answer: A

NEW QUESTION 275

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 276

In what portion of a project are risk and opportunities greatest and require intense planning and anticipation of risk events?

- A. Planning
- B. Executing
- C. Closing
- D. Initiating

Answer: D

NEW QUESTION 279

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 284

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 285

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 289

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 290

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 294

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 297

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 300

Which of the following is not a part of Identify Risks process?

- A. Decision tree diagram
- B. Cause and effect diagram
- C. Influence diagram
- D. System or process flow chart

Answer: A

NEW QUESTION 305

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 308

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 310

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 311

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

- A. Authorizing official

- B. Information system owner
- C. Chief information officer
- D. Common control provider

Answer: B

NEW QUESTION 313

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 316

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 319

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

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

Answer: B

NEW QUESTION 321

Which of the following NIST documents defines impact?

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

Answer: D

NEW QUESTION 326

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

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

Answer: D

NEW QUESTION 327

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 329

Management wants you to create a visual diagram of what resources will be utilized in the project deliverables. What type of a chart is management asking you to create?

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

Answer: C

NEW QUESTION 331

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 333

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 334

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

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

Answer: A

NEW QUESTION 339

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 342

Which of the following RMF phases is known as risk analysis?

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

Answer: C

NEW QUESTION 346

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 351

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 352

.....

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/>