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 assessment methodologies defines a six-step technical security evaluation?

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

Answer: B

NEW QUESTION 4
Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

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

Answer: B

NEW QUESTION 5
Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

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

Answer: D

NEW QUESTION 6
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan?
Each correct answer represents a part of the solution. Choose all that apply.

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

Answer: ABDE

NEW QUESTION 7
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 8
James work as an IT systems personnel in SoftTech Inc. He performs the following tasks: Runs regular backups and routine tests of the validity of the backup data.
Performs data restoration from the backups whenever required.
Maintains the retained records in accordance with the established information classification policy.
What is the role played by James in the organization?

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

Answer: D

NEW QUESTION 9
Which of the following refers to the ability to ensure that the data is not modified or tampered with?

A. Confidentiality
B. Availability
C. Integrity
D. Non-repudiation

Answer: C

NEW QUESTION 10
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 10
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 12
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 13
You are the project manager of the NNH Project. In this project you have created a contingency response that the schedule performance index should be less than 0.93. The NHH Project has a budget at completion of $945,000 and is 45 percent complete though the project should be 49 percent complete. The project has spent $455,897 to reach the 45 percent complete milestone.
What is the project's schedule performance index?

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

Answer: B

NEW QUESTION 17

A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Security law
B. Privacy law
C. Copyright law
D. Trademark law

Answer: B

NEW QUESTION 22
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 23
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 28
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 31
Which of the following are included in Physical Controls?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABEF

NEW QUESTION 35
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 preservesthe 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 36
You work as a project manager for BlueWell Inc. You are preparing to plan risk responses for your project with your team. How many risk response types are available for a negative risk event in the project?

A. Seven
B. Three
C. Four
D. One

Answer: C

NEW QUESTION 37
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 42
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 47
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 50
You work as the project manager for Bluewell Inc. You are working on NGQQ Projectyou??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 55
Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

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

Answer: A

NEW QUESTION 56
You work as a project manager for BlueWell Inc. Management has asked you to work with the key project stakeholder to analyze the risk events you have identified in the project. They would like you to analyze the project risks with a goal of improving the project's performance as a whole.
What approach can you use to achieve the goal of improving the project's performance through risk analysis with your project stakeholders?

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

Answer: B

NEW QUESTION 60
There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

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

Answer: A

NEW QUESTION 64
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 67
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 72
Sammy is the project manager for her organization. She would like to rate each risk based on its probability and affect on time, cost, and scope. Harry, a project team member, has never done this before and thinks Sammy is wrong to attempt this approach. Harry says that an accumulative risk score should be created, not three separate risk scores. Who is correct in this scenario?

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

Answer: A

NEW QUESTION 77
Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

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

Answer: A

NEW QUESTION 79
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 84
Mary is the project manager of the HGH Project for her company. She and her project team have agreed that if the vendor is late by more than ten days they will cancel the order and hire the NBG Company to fulfill the order. The NBG Company can guarantee orders within three days, but the costs of their products are significantly more expensive than the current vendor. What type of a response strategy is this?

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

Answer: C

NEW QUESTION 89
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 90
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 95
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 98
ISO 17799 has two parts. The first part is an implementation guide with guidelines on how to build a comprehensive information security infrastructure and the second part is an auditing guide based on requirements that must be met for an organization to be deemed compliant with ISO 17799. What are the ISO 17799 domains?
Each correct answer represents a complete solution. Choose all that apply.

A. Information security policy for the organization
B. Personnel security
C. Business continuity management
D. System architecture management
E. System development and maintenance

Answer: ABCE

NEW QUESTION 101
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 isthe 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 103
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 bethe 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 revealrisks.
D. Poorly written requirements will reveal inconsistencies in the project plans and documents.

Answer: A

NEW QUESTION 104
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 106
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 109
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 110
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test?
Each correct answer represents a complete solution. Choose all that apply.

A. Race conditions
B. Social engineering
C. Information system architectures
D. Buffer overflows
E. Kernel flaws
F. Trojan horses
G. File and directory permissions

Answer: ABDEFG

NEW QUESTION 111
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 116
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 120
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 125
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 126
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 131
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 136
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 140
Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

A. Secret information
B. Top Secret information
C. Confidential information
D. Unclassified information

Answer: B

NEW QUESTION 141
Nancy is the project manager of the NHH project. She and the project team have identified a significant risk in the project during the qualitative risk analysis process. Bob is familiar with the technology that the risk is affecting and proposes to Nancy a solution to the risk event. Nancy tells Bob that she has noted his response, but the risk really needs to pass through the quantitative risk analysis process before creating responses. Bob disagrees and ensures Nancy that his response is most appropriate for the identified risk. Who is correct in this scenario?

A. Bob is correc
B. Bob is familiar with the technology and the risk event so his response should be implemented.
C. Nancy is correc
D. Because Nancy is the project manager she can determine the correct procedures for risk analysis and risk response
E. In addition, she has noted the risk response that Bob recommends.
F. Nancy is correc
G. All risks of significant probability and impact should pass the quantitative risk analysis process before risk responses are created.
H. Bob is correc
I. Not all riskevents have to pass the quantitative risk analysis process to develop effective risk responses.

Answer: D

NEW QUESTION 145
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 146
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 150
A high-profile, high-priority project within your organization is being created. Management wants you to pay special attention to the project risks and do all that you can to ensure that all of the risks are identified early in the project. Management has to ensure that this project succeeds.
Management's risk aversion in this project is associated with what term?

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

Answer: A

NEW QUESTION 155
Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

A. Safeguard
B. Single Loss Expectancy (SLE)
C. Exposure Factor (EF)
D. Annualized Rate of Occurrence (ARO)

Answer: D

NEW QUESTION 158
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 160
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 162
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 164
Gary is the project manager for his organization. He is working with the project stakeholders on the project requirements and how risks may affect their project. One of the stakeholders is confused about what constitutes risks in the project. Which of the following is the most accurate definition of a project risk?

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

Answer: C

NEW QUESTION 166
You work as a project manager for BlueWell Inc. You are about to complete the quantitative risk analysis process for your project. You can use three available tools and techniques to complete this process. Which one of the following is NOT a tool or technique that is appropriate for the quantitative risk analysis process?

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

Answer: D

NEW QUESTION 169
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 172
The Identify Risk process determines the risks that affect the project and document their characteristics. Why should the project team members be involved in the Identify Risk process?

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

Answer: C

NEW QUESTION 176
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 180
Which of the following risk responses delineates that the project plan will not be changed to deal with the risk?

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

Answer: A

NEW QUESTION 183
Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 184
Your organization has named you the project manager of the JKN Project. This project has a BAC of $1,500,000 and it is expected to last 18 months. Management has agreed that if the schedule baseline has a variance of more than five percent then you will need to crash the project. What happens when the project manager crashes a project?

A. Project costs will increase.
B. The amount of hours a resource can be used will diminish.

C. The projectwill take longer to complete, but risks will diminish.
D. Project risks will increase.

Answer: A

NEW QUESTION 188
Virginia is the project manager for her organization. She has hired a subject matter expert to interview the project stakeholders on certain identified risks within the project. The subject matter expert will assess the risk event with what specific goal in mind?

A. To determine the bias of the risk event based on each person interviewed
B. To determine the probability and cost of the risk event
C. To determine the validity of each risk event
D. To determine the level of probability and impact for each risk event

Answer: D

NEW QUESTION 191
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 193
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 198
Harry is a project manager of a software development project. In the early stages of planning, he and the stakeholders operated with the belief that the software they were developing would work with their organization's current computer operating system. Now that the project team has started developing the software it has become apparent that the software will not work with nearly half of the organization's computer operating systems. The incorrect belief Harry had in the software compatibility is an example of what in project management?

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

Answer: D

NEW QUESTION 202
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 206
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 208
Fred is the project manager of the CPS project. He is working with his project team to prioritize the identified risks within the CPS project. He and the team are prioritizing risks for further analysis or action by assessing and combining the risks probability of occurrence and impact.
What process is Fred completing?

A. Risk identification
B. Perform qualitative analysis
C. Perform quantitative analysis
D. Risk Breakdown Structure creation

Answer: B

NEW QUESTION 213
Certification and Accreditation (C&A or CnA) is a process for implementing information security.
Which of the following is the correct order of C&A phases in a DITSCAP assessment?

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

Answer: C

NEW QUESTION 214
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 217
You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

A. Qualitative risk analysis
B. Quantitative analysis
C. Historical information
D. Rolling wave planning

Answer: A

NEW QUESTION 220
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 222
Which of the following NIST documents includes components for penetration testing?

A. NIST SP 800-53
B. NIST SP 800-26
C. NIST SP 800-37
D. NIST SP 800-30

Answer: D

NEW QUESTION 227
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 231
Which of the following NIST publications defines impact?

A. NIST SP 800-41
B. NIST SP 800-37
C. NIST SP 800-30
D. NIST SP 800-53

Answer: C

NEW QUESTION 236
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 237
Which of the following relations correctly describes total risk?

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

Answer: A

NEW QUESTION 240
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 800-53A
B. NIST SP 800-66
C. NIST SP 800-41
D. NIST SP 800-37

Answer: A

NEW QUESTION 244
Tom is the project manager for his organization. In his project he has recently finished the risk response planning. He tells his manager that he will now need to update the cost and schedule baselines. Why would the risk response planning cause Tom the need to update the cost and schedule baselines?

A. New or omitted work as part of a risk response can cause changes to the cost and/or schedule baseline.
B. Risk responses protect the time and investment of the project.
C. Risk responses may take time and money to implement.
D. Baselines should not be updated, but refined through versions.

Answer: A

NEW QUESTION 248
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 252
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 256
Which of the following processes is described in the statement below?
"It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

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

Answer: B

NEW QUESTION 260
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 263
The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: CDE

NEW QUESTION 266
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 269
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 273
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 276
Which of the following statements about Discretionary Access Control List (DACL) is true?

A. It is a rule list containing access control entries.
B. It specifies whether an audit activity should be performed when an object attempts to access a resource.
C. It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.
D. It is a unique number that identifies a user, group, and computer account

Answer: C

NEW QUESTION 278
......

Relate Links

Contact us