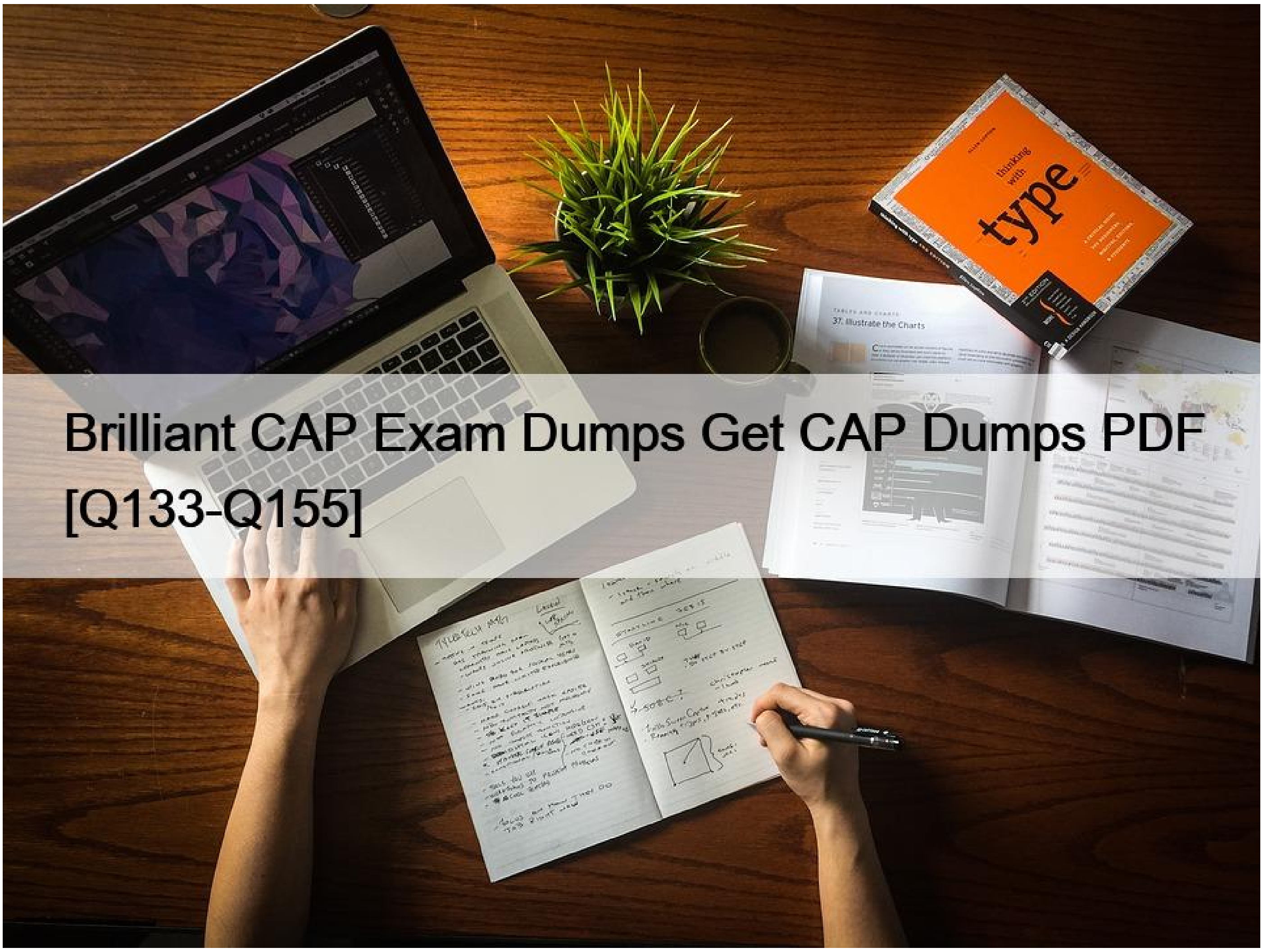
Brilliant CAP Exam Dumps Get CAP Dumps PDF [Q133-Q155



Brilliant CAP Exam Dumps Get CAP Dumps PDF
CAP Dumps PDF - CAP Real Exam Questions Answers

NEW QUESTION 133

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

Each correct answer represents a complete solution. Choose all that apply.
* BS 7799 Part 1 was adopted by ISO as ISO/IEC 27001 in November 2005.
* BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.
* BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards Institute (BSI) in 1995.
* BS 7799 Part 3 was published in 2005, covering risk analysis and management.

NEW QUESTION 134

The Project Risk Management knowledge area focuses on which of the following processes?

Each correct answer represents a complete solution. Choose all that apply.
* Potential Risk Monitoring
* Risk Management Planning
* Quantitative Risk Analysis
* Risk Monitoring and Control
Section: Volume B

NEW QUESTION 135

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&#8217;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?
* Mitigation
* Acceptance
* Transference
* Avoidance
Section: Volume B

NEW QUESTION 136

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?
* FIPS
* TCSEC
* SSAA
* FITSAF

NEW QUESTION 137

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&#8217;s concern, however, is that the priority list of these risk events are sorted in &#8220;high-risk,&#8221; &#8220;moderate-risk,&#8221; and &#8220;low-risk&#8221; 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&#8217;s reply to Tom?
* Risk may be listed by the responses inthe near-term
* Risks may be listed by categories
* Risks may be listed by the additional analysis and response
* Risks may be listed by priority separately for schedule, cost, and performance

NEW QUESTION 138

Which of the following guidance documents is useful in determining the impact level of a particular threat on agency systems?
* NIST SP 800-41
* NIST SP 800-37
* FIPS 199
* NIST SP 800-14

NEW QUESTION 139

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&#8217;s following the best practices for risk management?
* At every status meeting the project team project risk management is an agenda item.
* Project risk management happens at every milestone.
* Project risk management has been concluded with the project planning.
* Project risk management is scheduled for every month in the 18-month project.
Section: Volume B

NEW QUESTION 140

Which of the following approaches can be used to build a security program?

Each correct answer represents a complete solution. Choose all that apply.
* Bottom-Up Approach
* Right-Up Approach
* Top-Down Approach
* Left-Up Approach
Section: Volume B

NEW QUESTION 141

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?
* Four
* Seven
* Acceptance is the only risk response for positive risk events.
* Three

NEW QUESTION 142

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.
* System interaction
* Human interaction
* Equipment malfunction
* Inside and outside attacks
* Social status
* Physical damage

Section: Volume A

NEW QUESTION 143

Which of the following individuals is responsible for the final accreditation decision?
* Information System Owner
* Certification Agent
* User Representative
* Risk Executive
Section: Volume D

NEW QUESTION 144

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.
* Evaluating business objectives, security risks, user productivity, and functionality requirem ents
* Determining actual goals that are expected to be accomplished from a security program
* Defining steps to ensure that all the responsibilities are accounted for and properly address ed
* Determining objectives, scope, policies, priorities, standards, and strategies

NEW QUESTION 145

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

NEW QUESTION 146

What are the responsibilities of a system owner?

Each correct answer represents a complete solution. Choose all that apply.
* Integrates security considerations into application and system purchasing decisions and development projects.
* Ensures that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.
* Ensures that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on.
* Ensures that the necessary security controls are in place.

NEW QUESTION 147

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

&#8220;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.&#8221;

* Perform Quantitative Risk Analysis
* Perform Qualitative Risk Analysis
* Monitor and Control Risks
* Identify Risks

Section: Volume C

NEW QUESTION 148

An organization monitors the hard disks of its employees&#8217; computers from time to time. Which policy does this pertain to?

* Network security policy
* User password policy
* Backup policy
* Privacy policy

Section: Volume C

NEW QUESTION 149

The Project Risk Management knowledge area focuses on which of the following processes?

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

* Quantitative Risk Analysis
* Potential Risk Monitoring
* Risk Monitoring and Control
* Risk Management Planning

Section: Volume D

NEW QUESTION 150

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.

* Medium
* High
* Low
* Moderate

Section: Volume C

NEW QUESTION 151

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

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

NEW QUESTION 152

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

Each correct answer represents a complete solution. Choose all that apply.
* Configuration status accounting
* Configuration change control
* Configuration deployment
* Configuration audits
* Configuration identification
* Configuration implementation
Section: Volume C

NEW QUESTION 153

In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?
* Phase 2
* Phase 3
* Phase 1
* Phase 4

NEW QUESTION 154

Which of the following are included in Physical Controls?

Each correct answer represents a complete solution. Choose all that apply.
* Locking systems and removing unnecessary floppy or CD-ROM drives
* Environmental controls
* Password and resource management
* Identification and authentication methods
* Monitoring for intrusion
* Controlling individual access into the facility and different departments
Section: Volume A

NEW QUESTION 155

Which of the following NIST C&A documents is the guideline for identifying an information system as a National Security System?
* NIST SP 800-53
* NIST SP 800-59
* NIST SP 800-37
* NIST SP 800-53A
Section: Volume D

Explanation/Reference:

Valid CAP Test Answers & ISC CAP Exam PDF: https://www.exams4sures.com/ISC/CAP-practice-exam-dumps.html]