A. Information Systems Security Officer (ISSO)
B. Designated Approving Authority (DAA)
C. System Owner
D. Chief Information Security Officer (CISO)

Answer: B
Explanation:
The authorizing official is the senior manager responsible for approving the working of the information system. He is responsible for the risks of operating the information system within a known environment through the security accreditation phase. In many organizations, the authorizing official is also referred as approving/accrediting authority (DAA) or the Principal Approving Authority (PAA). Answer: C is incorrect. The system owner has the responsibility of informing the key officials within the organization of the requirements for a security C&A of the information system. He makes the resources available, and provides the relevant documents to support the process. Answer: A is incorrect. An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. Answer: D is incorrect. The CISO has the responsibility of carrying out the CIO's FISMA responsibilities. He manages the information security program functions.

QUESTION 148
DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP? Each correct answer represents a complete solution. Choose all that apply.

A. System Definition
B. Validation
C. Identification
D. Accreditation
E. Verification
F. Re-Accreditation

Answer: ABEF
Explanation:
The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle. DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases: 1.System Definition 2.Verification 3.Validation 4.Re-Accreditation

QUESTION 149
Which of the following are the goals of risk management? Each correct answer represents a

complete solution. Choose three.

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

Answer: ABD
Explanation:
There are three goals of risk management as follows: Identifying the risk Assessing the impact of potential threats Finding an economic balance between the impact of the risk and the cost of the countermeasure Answer: C is incorrect. Identifying the accused does not come under the scope of risk management.

QUESTION 150
NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews?

A. Comprehensive
B. Significant
C. Abbreviated
D. Substantial
Answer: C
Explanation:
Abbreviated interview consists of informal and ad hoc interviews. Answer: D is incorrect. Substantial interview consists of informal and structured interviews. Answer: A is incorrect. Comprehensive interview consists of formal and structured interviews. Answer: B is incorrect. There is no such type of interview in NIST SP 800-53A.

QUESTION 151
Which of the following are the principle duties performed by the BIOS during POST (power-on-self-test)? Each correct answer represents a part of the solution. Choose all that apply.

A. It provides a user interface for system's configuration.
B. It identifies, organizes, and selects boot devices.
C. It delegates control to other BIOS, if it is required.
D. It discovers size and verifies system memory.
E. It verifies the integrity of the BIOS code itself.
F. It interrupts the execution of all running programs.

Answer: ABCDE
Explanation:
The principle duties performed by the BIOS during POST (power-on-self-test) are as follows: It verifies the integrity of the BIOS code itself. It discovers size and verifies system memory. It discovers, initializes, and catalogs all system hardware. It delegates control to other BIOS if it is required. It provides a user interface for system's configuration. It identifies, organizes, and selects boot devices. It executes the bootstrap program. Answer: F is incorrect. The BIOS does not interrupt the execution of all running programs.

QUESTION 152
In which of the following architecture styles does a device receive input from connectors and

generate transformed outputs?

A. N-tiered
B. Heterogeneous
C. Pipes and filters
D. Layered

Answer: C
Explanation:
In the pipes and filters architecture style, a device receives input from connectors and generates transformed outputs. A pipeline has a series of processing elements in which the output of each element works as an input of the next element. A little amount of buffering is provided between the two successive elements.

QUESTION 153
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. Risk Breakdown Structure creation
C. Perform qualitative analysis
D. Perform quantitative analysis

Answer: C
Explanation:
Qualitative ranks the probability and impact and then helps the project manager and team to determine which risks need further analysis. Perform Qualitative Risk Analysis is the process of prioritizing risks for further analysis and action. It combines risks and their probability of occurrences and ranks them accordingly. It enables organizations to improve the project's performance by focusing on high-priority risks. Perform Qualitative Risk Analysis is usually a rapid and cost-effective means of establishing priorities for Plan Risk Responses. It also lays the foundation for Perform Quantitative Risk Analysis. Answer: A is incorrect. Risk identification precedes this activity. Answer: B is incorrect. This process does not describe the decomposition and organization of risks that you will complete in a risk breakdown structure.

Answer: D is incorrect. Quantitative analysis is the final step of risk analysis. Note the question tells you that Fred and the team will identify risks for additional analysis.

QUESTION 154
Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

A. Sensitive
B. Private
C. Unclassified
D. Confidential
E. Secret
F. Public

Answer: ABDF
Explanation:

The public or commercial data classification is also built upon a four-level model, which are as follows: Public Sensitive Private Confidential Each level (top to bottom) represents an increasing level of sensitivity. The public level is similar to unclassified level military classification system. This level of data should not cause any damage if disclosed. Sensitive is a higher level of classification than public level data. This level of data requires a greater level of protection to maintain confidentiality. The Private level of data is intended for company use only. Disclosure of this level of data can damage the company. The Confidential level of data is considered very sensitive and is intended for internal use only. Disclosure of this level of data can cause serious damage to the company. Answer: C and E are incorrect. Unclassified and secret are the levels of military data classification.

QUESTION 155
Which of the following statements are true about declarative security? Each correct answer represents a complete solution. Choose all that apply.

A. It is employed in a layer that relies outside of the software code or uses attributes of the code.
B. It applies the security policies on the software applications at their runtime.
C. In this security, authentication decisions are made based on the business logic.
D. In this security, the security decisions are based on explicit statements.

Answer: ABD
Explanation:
Declarative security applies the security policies on the software applications at their runtime. In this type of security, the security decisions are based on explicit statements that confine security behavior. Declarative security applies security permissions that are required for the software application to access the local resources and provides role-based access control to an individual software component and software application. It is employed in a layer that relies outside of the software code or uses attributes of the code. Answer: C is incorrect. In declarative security, authentication decisions are coarse-grained in nature from an operational or external security perspective.

QUESTION 156
What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?

A. Risk analysis plan
B. Staffing management plan
C. Risk management plan
D. Human resource management plan

Answer: C
Explanation:
The risk management plan defines how risks will be identified, analyzed, responded to, and then monitored and controlled regardless of the structure of the organization. Answer: D is incorrect. The human resources management plan does define how risks will be analyzed. Answer: B is incorrect. The staffing management plan does define how risks will be analyzed. Answer: A is incorrect. The risk analysis plan does define how risks will be analyzed.

QUESTION 157
The DoD 8500 policy series represents the Department's information assurance strategy. Which of the following objectives are defined by the DoD 8500 series? Each correct answer represents a complete solution. Choose all that apply.

A. Defending systems
B. Providing IA Certification and Accreditation
C. Providing command and control and situational awareness
D. Protecting information

Answer: ACD
Explanation:
The various objectives of the DoD 8500 series are as follows: Protecting information Defending systems Providing command and control and situational awareness Making sure that the information assurance is integrated into processes Increasing security awareness throughout the DoD's workforce

QUESTION 158
Which of the following vulnerabilities occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions?

A. Insecure cryptographic storage
B. Malicious file execution
C. Insecure communication
D. Injection flaw

Answer: B
Explanation:
Malicious file execution is a vulnerability that occurs when an application directly uses or concatenates potentially hostile input with data file or stream functions. This leads to arbitrary remote and hostile data being included, processed, and invoked by the Web server. Malicious file execution can be prevented by using an indirect object reference map, input validation, or explicit taint checking mechanism. Answer: D is incorrect. Injection flaw occurs when data is sent to an interpreter as a part of command or query. Answer: A is incorrect. Insecure cryptographic storage occurs when applications have failed to encrypt data. Answer: C is incorrect. Insecure communication occurs when applications have failed to encrypt network traffic.

QUESTION 159
Which of the following are the primary functions of configuration management? Each correct answer represents a complete solution. Choose all that apply.

A. It removes the risk event entirely by adding additional steps to avoid the event.
B. It ensures that the change is implemented in a sequential manner through formalized testing.
C. It reduces the negative impact that the change might have had on the computing services and resources.
D. It analyzes the effect of the change that is implemented on the system.

Answer: BCD
Explanation:
The primary functions of configuration management are as follows: It ensures that the change is implemented in a sequential manner through formalized testing. It ensures that the user base is informed of the future change. It analyzes the effect of the change that is implemented on the system. It reduces the negative impact that the change might have had on the computing services and resources. Answer: A is incorrect. It is not one of the primary functions of configuration management. It is the function of risk avoidance.