Latest Version: 6

Question: 1

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

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

Answer: A

Explanation:
The following are the five levels of FITSAF based on SEI's Capability Maturity Model (CMM):
Level 1: The first level reflects that an asset has documented a security policy.
Level 2: The second level shows that the asset has documented procedures and controls to implement the policy.
Level 3: The third level indicates that these procedures and controls have been implemented.
Level 4: The fourth level shows that the procedures and controls are tested and reviewed.
Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

Question: 2

Which of the following is a type of security management for computers and networks in order to identify
security breaches?

A. IPS
B. IDS
C. ASA
D. EAP

Answer: B

Explanation:
Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to

as scanning), which is a technology developed to assess the security of a computer system or network.
Intrusion detection functions include the following:
Monitoring and analyzing both user and system activities
Analyzing system configurations and vulnerabilities
Assessing system and file integrity
Ability to recognize patterns typical of attacks
Analysis of abnormal activity patterns
Tracking user policy violations
Answer option A is incorrect. An intrusion prevention system (IPS) is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in realtime,
to block or prevent those activities. When an attack is detected, the IPS can drop the offending packets while still allowing all other traffic to pass.
Answer option C is incorrect. Adaptive Security Appliance (ASA) is a new generation of network security hardware of Cisco. ASA hardware acts as a firewall, in other security roles, and in a combination of roles. The Cisco ASA includes the following components:
Anti-x: Anti-x includes whole class of security tools such as Anti-virus, Anti-spyware, Anti-spam, etc.
Intrusion Detection and Prevention: Intrusion Detection and Prevention includes tools such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for sophisticated kinds of attacks.
Note: Earlier Cisco sold firewalls with the proprietary name PIX firewall. ASA is the new edition of security solutions by Cisco.
Answer option D is incorrect. Extensible Authentication Protocol, or EAP, is a universal authentication framework frequently used in wireless networks and Point-to-Point connections. It is defined in RFC 3748, which has been updated by RFC 5247. Although the EAP protocol is not limited to wireless LANs and can be used for wired LAN authentication, it is most often used in wireless LANs. The WPA and WPA2
standard has officially adopted five EAP types as its official authentication mechanism. EAP is an authentication framework, not a specific authentication mechanism. The EAP provides some common functions and a negotiation of the desired authentication mechanism.

Question: 3

Which of the following types of firewalls increases the security of data packets by remembering the state
of connection at the network and the session layers as they pass through the filter?

A. Stateless packet filter firewall
B. PIX firewall
C. Stateful packet filter firewall
D. Virtual firewall

Answer: C

Explanation:
A stateful packet filter firewall maintains context about active sessions, and uses that "state information"

to speed packet processing. It increases the security of data packets by remembering the state of connection at the network and the session layers as the packets pass through the filter.
Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections.
If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing. PF (Packet Filter, also written pf) is a BSD licensed stateful packet filter, a central piece of software for firewalling. It is comparable to iptables, ipfw and ipfilter. PF is developed on OpenBSD, but has been ported to many other operating systems.
Answer option A is incorrect. A stateless packet filter firewall separately analyses incoming packets independently of the TCP connection or UDP data stream they belong to. It requires less memory, and can be faster for simple filters that require less time to filter than to look up a session. It may also be necessary for filtering stateless network protocols that have no concept of a session. However, it cannot make more complex decisions based on what stage communications between hosts have reached. It decides whether to allow a packet to traverse the firewall based on the header of the packet, without regard to past traffic through the firewall.
Stateless IP filters are very inexpensive, and many are free. They are included with router configuration software or are included with most Open Source operating systems.
Answer option B is incorrect. The PIX firewall is a Cisco product that performs VPN and firewall functions. This product comes in different models according to the requirements. Cisco's PIX firewall models such as PIX 501, 506 and 506E provide a firewall solution for small office environments. Cisco PIX 515, 515E, 525, etc. are widely used in medium and large enterprises. These days Adaptive Security Appliances (ASA) is used instead of PIX firewalls.
Answer option D is incorrect. A virtual firewall (VF) is a network firewall service or appliance running entirely within a virtualized environment and which provides the usual packet filtering and monitoring provided via a physical network firewall. The VF can be realized as a traditional software firewall on a guest virtual machine already running, or it can be a purpose-built virtual security appliance designed with virtual network security in mind, or it can be a virtual switch with additional security capabilities, or it can be a managed kernel process running within the host hypervisor.

Question: 4

Which of the following federal laws is designed to protect computer data from theft?

A. Federal Information Security Management Act (FISMA)
B. Computer Fraud and Abuse Act (CFAA)
C. Government Information Security Reform Act (GISRA)
D. Computer Security Act

Answer: B

Explanation:
The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1984 intended to reduce cracking of computer systems and to address federal computer-related offenses. The Computer Fraud and Abuse Act (codified as 18 U.S.C. 1030) governs cases with a compelling federal interest, where

computers of the federal government or certain financial institutions are involved, where the crime itself
is interstate in nature, or computers used in interstate and foreign commerce.
It was amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. Section (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Computer Fraud and Abuse Act but also those who conspire to
do so.
Answer option A is incorrect. FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level.
According to FISMA, the term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. Answer option C is incorrect. The Government Information Security Reform Act (GISRA) addresses the information security program, evaluation, and reporting requirements for federal agencies. The basic requirement of this law is that the agencies should perform the periodic threat-based risk assessments for systems and data. GISRA requires that the organizations should develop and execute risk-based, cost effective policies and procedures to provide guidance for security planning and implementation. GISRA's essential requisite is that the agencies should develop a process to guarantee that some corrective action has taken place to address the deficiencies. It also emphasizes that the agencies should provide training on security awareness and security responsibilities to agency personnel and information security personnel. Answer option D is incorrect. The Computer Security Act was passed by the United States Congress. It was passed to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems. It requires the creation of computer security plans, and the appropriate training of system users or owners where the systems house sensitive information.

Question: 5

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. ATM
B. RTM
C. CRO
D. DAA

Answer: B

Explanation:
RTM 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.
Answer option D is incorrect. The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for

operating a system at an acceptable level of risk. The DAA is responsible for implementing system security. The DAA can grant the accreditation and can determine that the system's risks are not at an acceptable level and the system is not ready to be operational.
Answer option A is incorrect. Asynchronous Transfer Mode (ATM) is a standardized digital data transmission technology. Asynchronous Transfer Mode is a cell-based switching technique that uses asynchronous time division multiplexing. It encodes data into small fixed-sized cells (cell relay) and provides data link layer services that run over OSI Layer 1 physical links. This differs from other technologies based on packet-switched networks (such as the Internet Protocol or Ethernet), in which variable sized packets (known as frames when referencing Layer 2) are used. ATM exposes properties from both circuit switched and small packet switched networking, making it suitable for wide area data networking as well as real-time media transport. ATM uses a connection-oriented model and establishes a virtual circuit between two endpoints before the actual data exchange begins. It provides medium to high bandwidth and low latency and jitter.
Answer option C is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach.

Question: 6

Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

A. Configuration Item Costing
B. Configuration Identification
C. Configuration Verification and Auditing
D. Configuration Status Accounting

Answer: A

Explanation:
Configuration item cost is not a valid activity for configuration management. Cost changes are managed by the cost change control system; configuration management is concerned with changes to the features and functions of the project deliverables.
Answer option B is incorrect. Configuration identification is a valid configuration management activity; it is the definition, verification, documentation and labeling of the product's features.
Answer option D is incorrect. Configuration status accounting is a valid configuration management activity; it is the capturing, storing, and accessing configuration information.
Answer option C is incorrect. Configuration verification and auditing is a valid configuration management activity; it is the confirmation of the performance and function requirements.

Question: 7

Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?

A. Authorizing Official
B. Information system owner
C. Chief Information Officer (CIO)
D. Chief Risk Officer (CRO)

Answer: B

Explanation:
The Certification and Accreditation (C&A) process starts when an information system owner acknowledges that a system, group of systems, application, or site needs Accreditation. An information system owner might be an IT operations director, a security officer, or an IT operations manager. When the requirement for C&A is acknowledged, it is required to supervise the C&A process.
Answer option D is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach.
Answer option C is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.
Answer option A is incorrect. An Authorizing Official plays the role of an approver. The responsibilities of an Authorizing Official are as follows:
Ascertains the security posture of the organization's information system.Reviews security status reports and critical security documents.Determines the requirement of reauthorization and reauthorizes information systems when required.

Question: 8

Which of the following security controls is a set of layered security services that address communications
and data security problems in the emerging Internet and intranet application space?

A. Internet Protocol Security (IPSec)
B. Common data security architecture (CDSA)
C. File encryptors

D. Application program interface (API)

Answer: B

Explanation:
The Common data security architecture (CDSA) is a set of layered security services and cryptographic framework. It deals with the communications and data security problems in the emerging Internet and intranet application space. It presents an infrastructure for building cross-platform, interoperable, security-enabled applications for client-server environments.
Answer option D is incorrect. An application programming interface (API) is an interface implemented by a software program which enables it to interact with other software. It facilitates interaction between different software programs similar to the way the user interface facilitates interaction between humans and computers. An API is implemented by applications, libraries, and operating systems to determine their vocabularies and calling conventions, and is used to access their services. It may include specifications for routines, data structures, object classes, and protocols used to communicate between the consumer and the implementer of the API. Answer option C is incorrect. File encrptors offer confidentiality and integrity for individual files. It gives a means of authenticating a ?le's source, and allows the exchange of encrypted files between computers.
Answer option A is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver.

Question: 9

Which of the following protocols is used to establish a secure terminal to a remote network device?

A. WEP
B. SMTP
C. SSH
D. IPSec

Answer: C

Explanation:
The Secure Shell (SSH) protocol is used to establish a secure terminal to a remote network device.
Answer option A is incorrect. Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs). It has two components, authentication and encryption. It provides security, which is equivalent to wired networks, for wireless networks. WEP encrypts data on a wireless network by using a fixed secret key. WEP incorporates a checksum in each frame to provide protection against the attacks that attempt to reveal the key stream.
Answer option D is incorrect. Internet Protocol Security (IPSec) is a method of securing data. It secures traffic by using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender verification that ensures the certainty of the datagram's origin to the receiver.
Answer option B is incorrect. Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail

messages between servers. E-mailing systems use this protocol to send mails over the Internet. SMTP works on the application layer of the TCP/IP or OSI reference model. The SMTP client typically initiates a Transmission Control Protocol (TCP) connection to the SMTP server on the well-known port designated for SMTP, port number 25. However, e-mail clients require POP or IMAP to retrieve mails from e-mail servers.

Question: 10

Which of the following elements of Registration task 4 defines the system's external interfaces as well as the purpose of each external interface, and the relationship between the interface and the system?

A. System firmware
B. System software
C. System interface
D. System hardware

Answer: C

Explanation:
System interface defines the system's external interfaces as well as the purpose of each external interface, and the relationship between the interface and the system.
Answer option D is incorrect. System hardware defines the target hardware and its function.
Answer option B is incorrect. System software defines the database management system, operating system, and software applications, and how they will be used.
Answer option A is incorrect. System firmware defines the firmware stored permanently in a hardware device that allows reading and execution of the software, but not writing or transforming it.

Question: 11

Which of the following guidelines is recommended for engineering, protecting, managing, processing, and controlling national security and sensitive (although unclassified) information?

A. Federal Information Processing Standard (FIPS)
B. Special Publication (SP)
C. NISTIRs (Internal Reports)
D. DIACAP by the United States Department of Defense (DoD)

Answer: B

Explanation:
The Special Publication (SP) is the guideline that is recommended for engineering, protecting, managing, processing, and controlling national security and sensitive (although unclassified) information. Answer option D is incorrect. 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. The DIACAP process is different from DITSCAP or NIACAP. Its overall process is similar to other C&A activities. The DIACAP process consists of five phases, which are as follows:
1.Initiate and Plan IA C&A. This phase consists of the following activities:
Register system with DoD Component IA Program.
Assign IA controls.
Assemble DIACAP team.
Develop DIACAP strategy.
Initiate IA implementation plan.
2.Implement and Validate Assigned IA Controls: This phase consists of the following activities:
Execute and update IA implementation plan. Conduct validation activities. Combine validation results in DIACAP scorecard. 3.Make Certification Determination and Accreditation Decisions: This phase consists of the following activities:
Analyze residual risk.Issue certification determination.Make accreditation decision.
4.Maintain Authority to Operate and Conduct Reviews: This phase consists of the following activities:
Initiate and update lifecycle implementation plan for IA controls.
Maintain situational awareness.Maintain IA posture.
5.Decommission System: This phase consists of the following activities:
Conduct activities related to the disposition of the system data and objects.
Answer option A is incorrect. FIPS emphasizes on design, implementation, and approval of cryptographicalgorithms.Answer option C is incorrect. NISTIRs (Internal Reports) illustrate the study of a technical nature of interest to focused audience. NISTIRs consist of interim or final reports on work made
by NIST for external sponsors, including government and non-government sponsors.

Question: 12

Which of the following Security Control Assessment Tasks gathers the documentation and supporting materials essential for the assessment of the security controls in the information system?

A. Security Control Assessment Task 4
B. Security Control Assessment Task 3
C. Security Control Assessment Task 1
D. Security Control Assessment Task 2

Answer: C

Explanation:
Security Control Assessment Task 1 gathers the documentation and supporting materials essential for the assessment of the security controls in the information system.
Answer option D is incorrect. Security Control Assessment Task 2 develops methods and procedures.
Answer option B is incorrect. Security Control Assessment Task 3 evaluates the operational, technical, and the management security controls of the information system using the techniques and measures selected or developed.

Answer option A is incorrect. Security Control Assessment Task 4 prepares the final security assessment report.

Question: 13

Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process?

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

Answer: C

Explanation:
A Common Control Provider plays the role of a monitor. The responsibilities of a Common Control Provider are as follows:
Develops a continuous monitoring scheme for the assigned common controls.
Takes part in the organization's configuration management process.
Establishes a stock of components associated with the common controls.
Performs security impact analysis on the changes that affect the common controls.
Performs security assessments of the common security controls.
Creates and submits security status reports to the defined organizations.
Updates critical security documents and provides it to information system owners and other leaders.
Performs remediation activities to maintain current authorization status.
Answer option A is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the
most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.
Answer option B is incorrect. An Authorizing Official plays the role of an approver. The responsibilities of an Authorizing Official are as follows:
Ascertains the security posture of the organization's information system.
Reviews security status reports and critical security documents.Determines the requirement of reauthorization and reauthorizes information systems when required.
Answer option D is incorrect. A Senior Agency Information Security Officer plays the role of a coordinator. The responsibilities of a Senior Agency Information Security Officer are as follows:
Establishes and implements the organization's continuous monitoring program.
Develops organizational guidance and configuration guidance for continuous monitoring of information systems and organization's information technologies respectively.
Consolidates and analyzes Plans of Action and Milestones (POAM) to decide organizational security weakness and inadequacy. Develops automated tools to support security authorization and continuousmonitoring.Provides training on the organization's continuous monitoring process.
Provides help to information system owners to develop and implement continuous monitoring.

Question: 14

Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?

A. Certification and accreditation (C&A)
B. Risk Management
C. Information systems security engineering (ISSE)
D. Information Assurance (IA)

Answer: A

Explanation:
Certification and accreditation (C&A) is a set of processes that culminate in an agreement between key players that a system in its current configuration and operation provides adequate protection controls. 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. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3.
Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Answer option B is incorrect. Risk management is a set of processes that ensures a risk-based approach is used to determine adequate, cost-effective security for a system.
Answer option D is incorrect. Information assurance (IA) is the process of organizing and monitoring information-related risks. It ensures that only the approved users have access to the approved information at the approved time. IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and nonrepudiation.
These objectives are applicable whether the information is in storage, processing, or transit, and whether threatened by an attack.
Answer option C is incorrect. ISSE is a set of processes and solutions used during all phases of a system's life cycle to meet the system's information protection needs.

Question: 15

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. Security operations
B. Continue to review and refine the SSAA
C. Change management
D. Compliance validation
E. System operations
F. Maintenance of the SSAA

Answer: E, A, F, C,

and D
Explanation:
The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase 3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this phase are as follows:
System operations
Security operations
Maintenance of the SSAA
Change management
Compliance validation
Answer option B is incorrect. It is a Phase 3 activity.

Question: 16

Which of the following email lists is written for the technical audiences, and provides weekly summaries of security issues, new vulnerabilities, potential impact, patches and workarounds, as well as the actions recommended to mitigate risk?

A. Cyber Security Tip
B. Cyber Security Alert
C. Cyber Security Bulletin
D. Technical Cyber Security Alert

Answer: C

Explanation:
The various free email lists are as follows:
Cyber Security Bulletins: This type of email list is written for the technical audiences. The Cyber Security Bulletins present the weekly summaries of security issues, new vulnerabilities, potential impact, patches and workarounds, and actions recommended mitigating risk.
Technical Cyber Security Alerts: This type of email list is written for the technical audiences. The Cyber Security Alerts give the timely information about current security issues, vulnerabilities, and exploits.
Cyber Security Alerts: This type of email list is written for non-technical home and corporate computer users. The Cyber Security Alerts

give the timely information about security issues, vulnerabilities, and exploits currently occurring.
Cyber Security Tips: This type of email list is written for non-technical home and corporate computer users. The bi-weekly Cyber
Security Tips gives information on computer security best practices.

Question: 17

Which of the following tasks obtains the customer agreement in planning the technical effort?

A. Task 9
B. Task 11
C. Task 8
D. Task 10

Answer: B

Explanation:
The various tasks performed in Plan the Effort process are as follows:
Task 1: Estimate project scope.
Task 2: Identify resources and availability.
Task 3: Identify roles and responsibilities.
Task 4: Estimate project costs.
Task 5: Develop project schedule.
Task 6: Identify technical activities.
Task 7: Identify deliverables.
Task 8: Define management interfaces.
Task 9: Prepare technical management plan.
Task 10: Review project plan.
Task 11: Obtain customer agreement.

Question: 18

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

Answer: D, E, F, A and

B
Explanation:

NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows:
NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems.
NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems.
NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security
controls in Federal Information System.
NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System.
NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.
Answer option C is incorrect. There is no such type of NIST document.

Question: 19

Which of the following elements are described by the functional requirements task?
Each correct answer represents a complete solution. Choose all that apply.

A. Coverage
B. Accuracy
C. Quality
D. Quantity

Answer: D, C, and A

Explanation:
The functional requirements categorize the different functions that the system will need to perform in order to gather the documented mission/business needs. The functional requirements describe the elements such as quantity, quality, coverage, timelines, and availability. Answer option B is incorrect. The
performance requirements comprise of speed, throughput, accuracy, humidity tolerances, mechanical stresses such as vibrations or noises.

Question: 20

Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality?

A. Information Protection Policy (IPP)
B. IMM
C. System Security Context
D. CONOPS

Answer: A

Explanation:
The Information Protection Policy (IPP) is defined as a source document, which is most useful for the ISSE
when classifying the needed security functionality. The IPP document consists of the threats to the information management and the security services and controls needed to respond to those threats.
Answer option B is incorrect. The IMM is the source document describing the customer's needs based on
identifying users, processes, and information. Answer option C is incorrect. The System Security Context is the output of SE and ISSEP. It is the translation of the requirements into system parameters and possible measurement concepts that meet the defined requirements. Answer option D is incorrect. The Concept of Operations (CONOPS) is a document describing the characteristics of a proposed system from
the viewpoint of an individual who will use that system. It is used to communicate the quantitative and qualitative system characteristics to all stakeholders. CONOPS are widely used in the military or in government services, as well as other fields. A CONOPS generally evolves from a concept and is a description of how a set of capabilities may be employed to achieve desired objectives or a particular end state for a specific scenario.