Information Systems Security Engineering Professional

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. A. Level 4

B. B. Level 5

C. C. Level 1

D. D. Level 2

E. E. Level 3

Answer(s): A

---

2. QUESTION NO: 2

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

A. A. IPS

B. B. IDS

C. C. ASA

D. D. EAP

Answer(s): B

---

3. QUESTION NO: 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. A. Stateless packet filter firewall

B. B. PIX firewall

C. C. Stateful packet filter firewall

D. D. Virtual firewall

Answer(s): C

---

4. QUESTION NO: 4

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

A. A. Federal Information Security Management Act (FISMA)

B. B. Computer Fraud and Abuse Act (CFAA)

C. C. Government Information Security Reform Act (GISRA)

D. D. Computer Security Act

Answer(s): B

---

5. QUESTION NO: 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. A. ATM

B. B. RTM

C. C. CRO

D. D. DAA

Answer(s): B

---

6. QUESTION NO: 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. A. Configuration Item Costing

B. B. Configuration Identification

C. C. Configuration Verification and Auditing

D. D. Configuration Status Accounting

Answer(s): A

---

7. QUESTION NO: 7
Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?

A. A. Authorizing Official

B. B. Information system owner

C. C. Chief Information Officer (CIO)
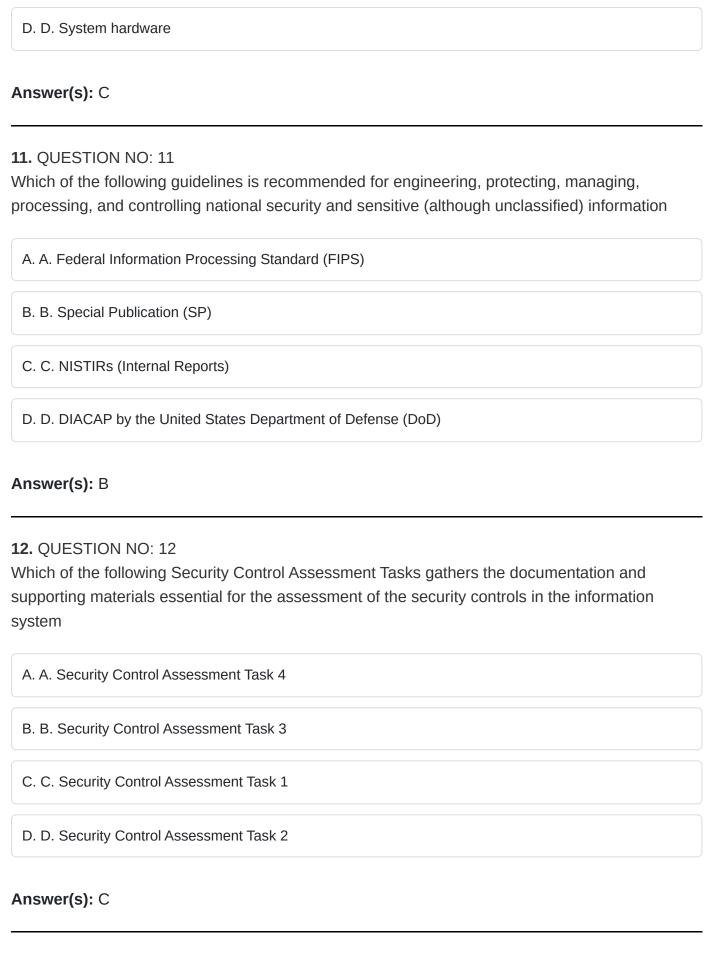
D. D. Chief Risk Officer (CRO)

Answer(s): B

---

8. QUESTION NO: 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. A. Internet Protocol Security (IPSec)

B. B. Common data security architecture (CDSA)

C. C. File encryptors

D. D. Application program interface (API)

Answer(s): B

---

9. QUESTION NO: 9

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

A. A. WEP

B. B. SMTP

C. C. SSH

D. D. IPSec

Answer(s): C

---

10. QUESTION NO: 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. A. System firmware

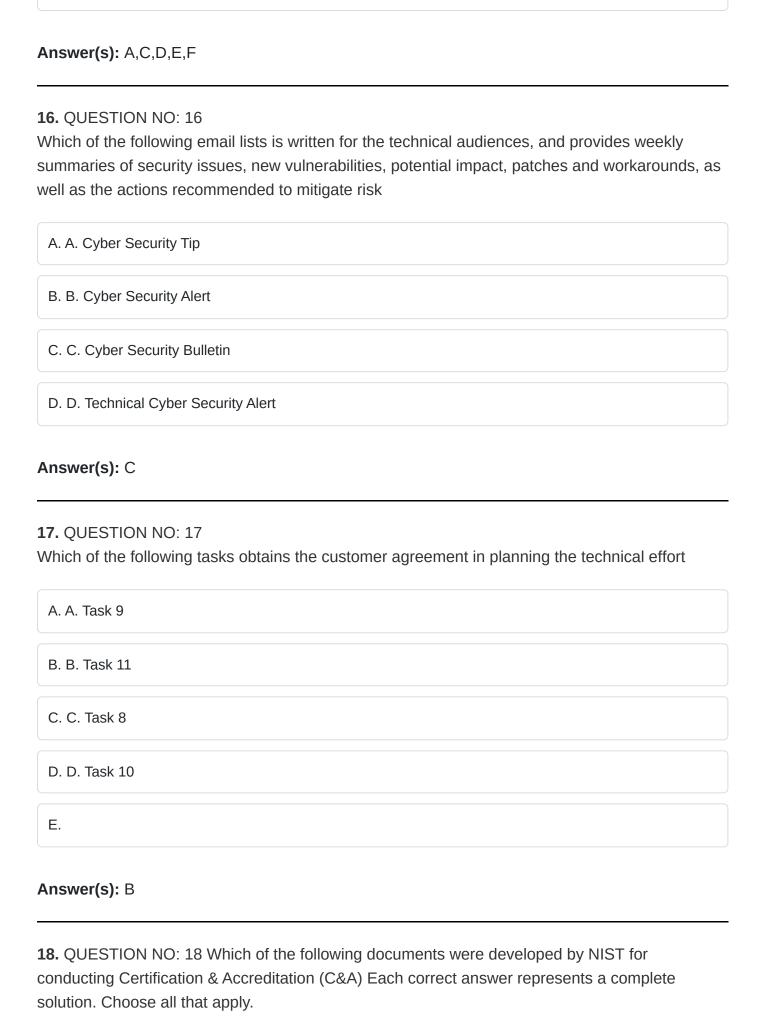B. B. System software

C. C. System interface

D. D. System hardware

Answer(s): C

---

11. QUESTION NO: 11

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

A. A. Federal Information Processing Standard (FIPS)

B. B. Special Publication (SP)

C. C. NISTIRs (Internal Reports)

D. D. DIACAP by the United States Department of Defense (DoD)

Answer(s): B

---

12. QUESTION NO: 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. A. Security Control Assessment Task 4

B. B. Security Control Assessment Task 3

C. C. Security Control Assessment Task 1

D. D. Security Control Assessment Task 2

Answer(s): C

---

13. QUESTION NO: 13

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

A. A. Chief Information Officer

B. B. Authorizing Official

C. C. Common Control Provider

D. D. Senior Agency Information Security Officer

Answer(s): C

---

14. QUESTION NO: 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. A. Certification and accreditation (C&A)

B. B. Risk Management

C. C. Information systems security engineering (ISSE)

D. D. Information Assurance (IA)

Answer(s): A

---

15. QUESTION NO: 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. A. Security operations

B. B. Continue to review and refine the SSAA

C. C. Change management

D. D. Compliance validationE. System operations

Answer(s): A,C,D,E,F

---

16. QUESTION NO: 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. A. Cyber Security Tip

B. B. Cyber Security Alert

C. C. Cyber Security Bulletin

D. D. Technical Cyber Security Alert

Answer(s): C

---

17. QUESTION NO: 17
Which of the following tasks obtains the customer agreement in planning the technical effort

A. A. Task 9

B. B. Task 11

C. C. Task 8

D. D. Task 10

E.

Answer(s): B

---

18. QUESTION NO: 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. A. NIST Special Publication 800-59

B. B. NIST Special Publication 800-60

C. C. NIST Special Publication 800-37A

D. D. NIST Special Publication 800-37

E. E. NIST Special Publication 800-53

F. F. NIST Special Publication 800-53A

Answer(s): A,B,D,E,F

---

19. QUESTION NO: 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. A. Coverage

B. B. Accuracy

C. C. Quality

D. D. Quantity

Answer(s): A,C,D

---

20. QUESTION NO: 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. A. Information Protection Policy (IPP)

B. B. IMM

C. C. System Security Context

D. D. CONOPS

Answer(s): A