Certified in Governance, Risk, and Compliance

1. An authorization approach where multiple organizational officials either from the same organization or different organizations, have a shared interest in authorizing a system is known as:

A. Single authorization

B. Traditional authorization

C. Site authorization

D. Joint authorization

Answer(s): D

---

2. 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.

A. Privacy law

B. Trademark law

C. Copyright law

D. Security law

Answer(s): A

---

3. What are the four phases for interconnecting systems?

A. 1 - Establishing2 - Maintaining3 - Disconnecting4 - Evaluating

B. 1 - Planning2 - Establishing3 - Maintaining4 - Disconnecting

C. 1 - Planning2 - Establishing3 ?Maintaining4 - Monitoring

D. 1 - Planning2 - Maintaining3 ?Disconnecting4 - Providing

Answer(s): B

---

4. During which Risk Management Framework (RMF) step is the system security plan initially approved? Response:

A. RMF Step 5 Authorize Information System

B. RMF Step 3 Implement Security Controls

C. RMF Step 2 Select Security Controls

D. RMF Step 1 Categorize Information System

Answer(s): C

---

5. Which of the three-tiered approaches to risk management address risk at the IS security control level & their allocation?

A. Management Systems

B. Security System

C. Federal Systems

D. Information Systems

Answer(s): D

---

6. A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

A. Strength Exercise

B. Tabletop Exercise

C. Flexibility Exercise.

D. Resolution Exercise

Answer(s): B

---

7. Which NIST special configuration provides guidance on security-focused configuration management? Response:

A. NIST SP 800-37

B. NIST SP 800-30

C. NIST SP 800-137

D. NIST SP 800-128

Answer(s): D

---

8. Who provides oversight of activities of the system owner, who provides trend analysis to id problems that may impact security posture. From Enterprise perspective reports to AO and system owners on organization wide risks (ISSO, CISO, ISO).

A. ISO

B. AODR

C. CISO

D. ISSO

Answer(s): C

---

9. Which of the following is a goal of Public Law?

A. Complete, reliable, and trustworthy information for Authorizing Officials

B. Ensure that Authorizing Officials do not have budgetary authority over the systems they provide authorization decisions for thus preventing a conflict of interest.

C. Compartmentalization of security information to increase security within departments of the government

D. Reduce cost of security controls

Answer(s): A

---

10. Which NIST SP 800 series document is concerned with continuous monitoring of Federal Information Systems & organizations?

A. SP 800-26

B. SP 800-144

C. SP 800-137

D. SP 800-64

Answer(s): C

---

11. Which if the following is an example of the test assessment method? Response:

A. Reviewing the most recent scan reports

B. Conducting a vulnerability scan on web applications

C. Reading vulnerability scan policies and procedures

D. Asking administrators about the scanning process

Answer(s): B

---

12. Which NIST SP is a Guide for Conducting.

A. NIST SP 800-37

B. NIST SP 800-30

C. NIST SP 800-50

D. NIST SP 800-58

Answer(s): B

---

13. An occurrence that actually jeopardizes the CIA of an information system or the information system processes that stores or transmits information or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

A. Data breach

B. Compromise

C. Incident

D. Event

Answer(s): C

---

14. The phase 3 of the Risk Management Framework (RMF) process is known as mitigation planning. Which of the following processes take place in phase 3?

A. Identify threats, vulnerabilities, and controls that will be evaluated.

B. Document and implement a mitigation plan.

C. Agree on a strategy to mitigate risks.

D. Evaluate mitigation progress and plan next assessment.

Answer(s): B,C,D

---

15. Which role has the primary responsibility to conduct ongoing assessments after an initial system authorization?

A. Information System Owner (ISO)

B. Security Control Assessor

C. Common Control Provider (CCP)

D. Authorizing Official (AO)

Answer(s): B

---

16. Another term used to refer to a Security Controls Assessment or security review; is? Response:

A. Security Test (ST)

B. Security Control

C. Security Test & Evaluation (ST&E)

D. Evaluation

Answer(s): C

---

17. The first item listed in the system security plan is the system name and identifier. As required in OMB Circular A 11, each system should be assigned a name and unique identifier. The assignment of a unique identifier supports the agencys ability to do what?

A. Identify risks associated to location.

B. Create an RTM.

C. Collect agency information and security metrics specific to the system.

D. Establish budget auditability.

Answer(s): C

---

18. The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred.

A. Common Vulnerability and Exposures (CVE)

B. Business Continuity Plan (BCP)

C. Business Recovery/Disruption Plan (BRP)

D. Business Impact Analysis (BIA)

Answer(s): B

---

19. NIST SP 800-53 describes a family of controls as:

A. A grouping of control tests from NIST SP 800-53A that corresponds to a class of controls in NIST SP 800-53

B. A grouping of controls that when applied provides a complete protection package for a single network

C. A grouping of like controls covering the same subject

D. A grouping of interoperating controls from all three classes of controls

Answer(s): C

---

20. Which role in the security authorization process is responsible for organizational information systems? Response:

A. User representative

B. IS program manager

C. Designated authorizing official

D. Certification agent

Answer(s): C
