

## Risk Management Framework (RMF) for DoD IT – Concepts Quiz

**Instructions:** Select a, b, c, or d to indicate the choice that most closely fits the blank space in each statement.

1. \_\_\_\_\_ is the evaluation of a system's compliance with a defined set of security requirements.
  - a. Accreditation
  - b. Security Authorization
  - c. OMB A-130
  - d. Security Control Assessment
2. \_\_\_\_\_ is the *primary* consideration leading to a decision to authorize a system for operation.
  - a. Compliance with all applicable controls
  - b. Acceptability of risk
  - c. Cost to mitigate existing vulnerabilities
  - d. Mission need
3. The legacy terms "Certification" and "Accreditation" correspond to \_\_\_\_\_ and \_\_\_\_\_ of RMF.
  - a. Implement (3) and Assess (4)
  - b. Implement (3) and Authorize (5)
  - c. Assess (4) and Authorize (5)
  - d. There is no clear cut correspondence between C&A and RMF steps
4. The three fundamental objectives of information security are \_\_\_\_\_.
  - a. Confidentiality, Integrity, and Availability
  - b. Access control, Identification & Authentication, and Audit
  - c. Computer security, network security, and physical security
  - d. Non-repudiation, message integrity, and encryption
5. The Federal Information Security Management Act (FISMA) \_\_\_\_\_.
  - a. Applies to the entire federal government
  - b. Does not apply to DoD or intelligence community agencies
  - c. Applies to departments and agencies within the executive branch
  - d. Applies only to systems that store or process Privacy Act information
6. \_\_\_\_\_ is/are NOT a part of an agency's information security program as mandated by FISMA
  - a. Periodic risk assessments
  - b. Test and evaluation of security controls
  - c. Security awareness training
  - d. Quarterly software updates
7. The new step added in the NIST SP 800-37 R2 is \_\_\_\_\_.
  - a. Prepare – Organizational Level and System Level
  - b. Identifying the Authorizing Official or DAA
  - c. Development of the System Security Plan (SSP)
  - d. Allocating a budget for information security

## Risk Management Framework (RMF) for DoD IT – Concepts Quiz

8. What are the primary documents in an RMF Authorization package?
  - a. Security Plan, Risk Assessment, POA&M
  - b. Risk Assessment, Continuous Monitoring Strategy, POA&M
  - c. Security Plan, Security Assessment Report, POA&M
  - d. Concept of Operations, Contingency Plans, POA&M
9. NIST Special Publication (SP) 800-53 provides a catalog of security controls, while SP 800-53A provides \_\_\_\_\_.
  - a. Additional controls for national security systems and other special circumstances
  - b. Guidance on assigning controls based on the FIPS 199 system categorization
  - c. Guidance on assessment of security controls
  - d. A template for reporting the security controls status
10. The Risk Assessment Report quantifies system risks in terms of \_\_\_\_\_.
  - a. Threat level and vulnerability score
  - b. Effectiveness of system safeguards
  - c. A FIPS-certified risk management model
  - d. Likelihood and impact
11. The Plan of Action and Milestones (POA&M) is \_\_\_\_\_.
  - a. Comprised of items tied to risks identified in the Security Controls Assessment
  - b. A tracking tool for security improvements
  - c. A living document updated regularly throughout the system life cycle
  - d. All of the above
12. This document provides categorization guidance and security controls for national security systems:
  - a. NIST SP 800-37
  - b. CNSSI 1253
  - c. NIST SP 800-122
  - d. NIST SP 800-39
13. FISMA requires agencies to report annually on the state of their information security program to \_\_\_\_\_.
  - a. Congress
  - b. Office of Management and Budget (OMB)
  - c. General Accounting Office (GAO)
  - d. Department of Homeland Security (DHS)
14. NIST Special Publications (SP) contain \_\_\_\_\_.
  - a. Policy directives that are mandatory for all federal departments and agencies
  - b. Guidance that has been adopted and adapted by many federal agencies as the basis of their information security program
  - c. Recommended configuration settings for operating systems and databases
  - d. Instructions on FISMA reporting to OMB

## Risk Management Framework (RMF) for DoD IT – Concepts Quiz

15. Use of commercial security tools \_\_\_\_\_.  
a. Is mandated by FISMA and RMF  
b. Is prohibited in most federal agencies  
c. Can provide assistance in workflow management and other RMF activities  
d. Makes RMF a purely clerical task
16. Continuous Monitoring is \_\_\_\_\_.  
a. Addressed in RMF Step “Monitor”  
b. Addressed in all of the RMF steps  
c. Addressed in RMF Steps “Select” and “Monitor”  
d. Not specifically addressed in RMF
17. The Joint Task Force Transformation Initiative (JTFTI) is responsible for \_\_\_\_\_.  
a. Developing a “unified information security framework” for the federal government  
b. Integrating the Dept. of Defense and the Dept. of Homeland Security  
c. Assessing information systems in preparation for security authorization  
d. None of these; JTFTI is a fictional organization featured in a Hollywood movie
18. FISMA mandates review of security controls \_\_\_\_\_.  
a. Annually  
b. At least once every three years  
c. Quarterly  
d. Continuously
19. \_\_\_\_\_ is the assurance that information is not disclosed to unauthorized persons, processes, or devices.  
a. Integrity  
b. Confidentiality  
c. Non-repudiation  
d. Information Security
20. \_\_\_\_\_ is the document that provides an overview of the security requirements of a system and the controls in place or planned for meeting those requirements  
a. Plan of Action and Milestones  
b. System Concept of Operations  
c. Security Plan  
d. Risk Assessment