



Information security and IT risk management – Question bank

By Manish Agrawal, Alex Campoe and Eric Pierce

Chapter 2 – System Administration

1. The system administrator is the person responsible for

- a) Day-to-day operation of a technology system
- b) Writing , enforcing , and reviewing security-operating procedures
- c) Developing new technology systems
- d) Upgrading existing technology systems

Answer: (a)

2. The system security officer is the person responsible for

- a) Day-to-day operation of a technology system
- b) Writing , enforcing , and reviewing security-operating procedures
- c) Developing new technology systems
- d) Upgrading existing technology systems

Answer: (b)

3. Common system administration tasks include

- a) Developing software
- b) Purchasing hardware
- c) Updating software
- d) Customer service

Answer: (c)

4. System administration provides all of the following except

- a) Support services
- b) Reliable operations
- c) Efficient use of the system
- d) Project management

Answer: (d)

5. Cloud computing models include all of the following except

- a) Revenue as a service
- b) Infrastructure as a service
- c) Platform as a service
- d) Software as a service

Answer: (a)

6. A virtual machine

- a) Is another name for computers installed inside virtual reality gaming systems
- b) is a software container into which an operating system and applications can be installed
- c) Is the display device in virtual reality systems
- d) Is a machine in name only

Answer: (b)

7. Writing the necessary data in the appropriate locations on a computer's hard drive for running a software program is called

- a) Configuration
- b) Access control
- c) Installation
- d) User management

Answer: (c)

8. Selecting one among many possible combinations of features of a system is called

- a) User management
- b) Access control
- c) Installation
- d) Configuration

Answer: (d)

9. Limiting access to information system resources only to authorized users, programs, processes, or other systems is called

- a) Access control
- b) User management
- c) Installation

- d) Configuration

Answer: (a)

10. Defining the rights of organizational members to information in the organization is called

- a) Access control
- b) User management
- c) Installation
- d) Configuration

Answer: (b)

11. Listening and/or recording the activities of a system to maintain performance and security is called

- a) Access control
- b) User management
- c) Monitoring
- d) Configuration

Answer: (c)

12. The types of monitoring include

- a) Penetration testing and access control
- b) Health checking and log monitoring
- c) Nagios and log monitoring
- d) Reactive monitoring and pro-active testing

Answer: (d)

13. A part of a system whose failure will stop the entire system from working is a

- a) Single point of failure
- b) Redundancy
- c) Availability
- d) Nagios

Answer: (a)

14. A hot spare is a

- a) Single point of failure

- b) Redundant component that can replace a failed component with no downtime
- c) Spare components used to replace failed components as quickly as possible
- d) Popular component purchased when it is on sale

Answer: (b)

15. A cold spare is a

- a) Single point of failure
- b) Redundant component that can replace a failed component with no downtime
- c) Spare components used to replace failed components as quickly as possible
- d) Popular component purchased when it is on sale

Answer: (c)

16. Common functions offered by system utilities in the Windows world include

- a) Providing surplus capacity, to improve availability
- b) Replacing failed components with minimal downtime
- c) Automating the collection of music and other multimedia information
- d) Automating and auditing the installation and maintenance of software

Answer: (d)

17. UNIX was developed by

- a) Ken Thompson and Dennis Ritchie in 1969
- b) Bill Gates and Paul Allen in 1977
- c) Edgar F. Codd in 1970
- d) Bob Metcalfe in 1973

Answer: (a)

18. Redundancy is

- a) Availability of choices
- b) Surplus capacity, used to improve the reliability of a system
- c) Availability of multiple versions of a software
- d) Managing users in a domain

Answer: (b)

19. The domain controller in Active Directory

- a) Serves web pages in the domain

- b) Bills users in the domain
- c) Implements the active directory rules in the domain
- d) Installs updated on all computers in the domain

Answer: (c)

20. Active Directory

- a) Encourages computer users to perform physical activities throughout the day
- b) Adds icons to directories in Windows Explorer
- c) Improves search features in Windows computers
- d) Provides centralized user management and access control for computers

Answer: (d)

21. Linux is

- a) An operating system that behaves like UNIX, though it has an independent code base
- b) A different brand of UNIX
- c) A version of Windows
- d) A database system

Answer: (a)

22. Open source software is

- a) An operating system that behaves like UNIX
- b) Software in which anyone can modify the source code
- c) A version of Windows
- d) A hobby

Answer: (b)

23. Common functions of Linux System Administration utilities include

- a) Automated customer service
- b) Automated business processing
- c) Automated installation
- d) Automated marketing

Answer: (c)

24. Multiple versions of Unix exist because

- a) Availability of choices is good for customers

- b) Unix and Linux are not maintained
- c) Availability of versions improved the competitiveness of Unix against Windows
- d) AT&T licensed many institutions to create their own versions

Answer: (d)

25. A Linux distribution is

- a) A collection of open source utilities and software packaged with the Linux OS
- b) An older version of Linux
- c) A specific version of Linux, focused on competing with Microsoft
- d) The “official” version of Linux

Answer: (a)