1. The primary goals and objectives of security are contained within the CIA Triad
2. Without object integrity, confidentiality cannot be maintained
3. Integrity can be examined from three perspectives:
    a. Preventing unauthorized subjects from making modifications
    b. Preventing authorized subjects from making unauthorized modifications, such as mistakes
    c. Maintaining the internal and external consistency of objects so that their data is a correct and true reflection of the real world and any relationship with any child, peer, or parent object is valid, consistent, and verifiable
4. Availability depends on both integrity and confidentiality. Without integrity and confidentiality, availability cannot be maintained
5. Identification =>Authentication =>Authorization=>Auditing=>Accounting
6. Identification claiming an identity when attempting to access a secured area or system
7. Authentication proving that you are that identity
8. Authorization defining the allows and denials of resource and object access for a specific identity
9. Auditing recording a log of the events and activities related to the system and subjects
10. Accounting (aka accountability) reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions
11. The audit trails created by recording system events to logs can be used to evaluate the health and performance of a system.
12. Nonrepudiation prevents a subject from claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event
13. Nonrepudiation can be established using digital certificates, session identifiers, transaction logs, and numerous other transactional and access control mechanisms.
14. Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization.
15. Security governance is an attempt to emphasize thispoint by indicating that security needs to be managed and governed throughout the organization, not just in the IT department.
16. Security management planning ensures proper creation, implementation, and enforcement of a security policy.
17. A business case is usually a documented argument or stated position in order to define a need to make a decision or take some form of action.
18. The bottom-up approach is rarely used in organizations and is considered problematic in the IT industry.
19. The best security plan is useless without one key factor: approval by senior management. Without senior management's approval of and commitment to the security policy, the policy will not succeed.
20. The goal of change management is to ensure that any change does not lead to reduced or compromised security. Change management is also responsible for making it possible to roll back any change to a previous secured state.
21. Data classification, or categorization, is the primary means by which data is protected based on its need for secrecy, sensitivity, or confidentiality.
22. The primary objective of data classification schemes is to formalize and stratify the process of securing data based on assigned labels of importance and sensitivity.

23. The senior manager must sign off on all policy issues
24. The security professional has the functional responsibility for security, including writing the security policy and implementing it.
25. Data owner usually delegates the responsibility of the actual data management tasks to a data custodian.
26. Due diligence is practicing the activities that maintain the due care effort.
27. Senior management must show due care and due diligence to reduce their culpability and liability when a loss occurs.
28. A security policy is a document that defines the scope of security needed by the organization and discusses the assets that require protection and the extent to which security solutions should go to provide the necessary protection.
29. Standards define compulsory requirements for the homogenous use of hardware, software, technology, and security controls
30. A baseline defines a minimum level of security that every system throughout the organization must meet
31. Guidelines are the next element of the formalized security policy structure
32. A procedure is a detailed, step-by-step how-to document that describes the exact actions necessary to implement a specific security mechanism, control, or solution
33. Threat modeling is the security process where potential threats are identified, categorized,and analyzed.
34. Threat modelling two goals
    a. To reduce the number of security-related design and coding defects
    b. To reduce the severity of any remaining defects
35. STRIDE
    a. Spoofing
    b. Tampering
    c. Reduction
    d. Information Disclosure
    e. Denial of Services
    f. Elevation of Privilege
36. Evaluating third Party
    a. On-Site Assessment
    b. Document Exchange and Review Investigate
    c. Process/Policy Review