1. X.800 defines access control as the prevention of unauthorized use of a resource,  
including the prevention of use of a resource in an unauthorized manner.  
2. An independent review and examination of system records and activities in order to test for  
adequacy of system controls, to ensure compliance with established policy and operational  
procedures, to detect breaches in security, and to recommend any indicated changes in control,  
policy and procedures is a(n) audit.  
3. Role based access control controls access based on the roles that users have within the system  
and on rules stating what accesses are allowed to users in given roles.  
4. Discretionary access control controls access based on the identity of the requestor and on access  
rules stating what requestors are or are not allowed to do.  
5. The basic elements of access control are: subject, object and access right.  
6. Basic access control systems typically define three classes of subject: owner, group and  
world.  
7. A discretionary access control scheme is one in which an entity may be granted access rights  
that permit the entity, by its own volition, to enable another entity to access some resource.  
8. The super user ID is exempt from the usual file access control constraints and has system  
wide access.  
9. A session is a mapping between a user and an activated subset of the set of roles to which  
the user is assigned.  
10. Role hierarchies make use of the concept of inheritance to enable one role to implicitly  
include access rights associated with a subordinate role.  
11. A prerequisite dictates that a user can only be assigned to a particular role if it is already  
assigned to some other specified role and can be used to structure the implementation of the least  
privilege concept.  
12. \_\_\_\_\_\_\_\_\_\_ functions provide the capability to create, delete, and maintain RBAC elements  
and relations.  
13. The NIST model defines two types of role hierarchies: general role hierarchies and  
limited hierarchies.  
14. Static Separation of Duty enables the definition of a set of mutually exclusive roles, such  
that if a user is assigned to one role in the set, the user may not be assigned to any other role in the  
set.  
15. The administrative functions include the following: create a user session with a default set of  
active roles; add an active role to a session; delete a role from a session; and check if the session  
subject has permission to perform a request operation on an object.  
**Choose from the following concepts:**  
object,  
supporting system,