1. Computer Security is the protection afforded to an automated information system in order to attain  
the applicable objectives of preserving the integrity, availability, and confidentiality of  
information system resources.  
2. Confidentiality, Integrity, and Availability form what is often referred to as the CIA triad.  
3. A loss of availability is the disruption of access to or use of information or an information  
system.  
4. In the United States, student grade information is an asset whose confidentiality is regulated  
by the FERPA.  
5. A(n) attack is a threat that is carried out and, if successful, leads to an undesirable  
violation of security, or threat consequence.  
6. A(n) countermeasure is any means taken to deal with a security attack.  
7. Misappropriation and misuse are attacks that result in usurpation threat consequences.  
8. The assets of a computer system can be categorized as hardware, software, communication  
lines and networks, and data.  
9. Release of message contents and traffic analysis are two types of passive attacks.  
10. Replay, masquerade, modification of messages, and denial of service are example of  
active attacks.  
11. Establishing, maintaining, and implementing plans for emergency response, backup  
operations, and post disaster recovery for organizational information systems to ensure the  
availability of critical information resources and continuity of operations in emergency situations  
is a contingency plan.  
12. A(n) risk assessment is periodically assessing the risk to organizational operations,  
organizational assets, and individuals, resulting from the operation of organizational information  
systems and the associated processing, storage, or transmission or organizational information.  
13. The OSI security architecture focuses on security attacks, mechanisms and services.  
14. A digital signature is data appended to, or a cryptographic transformation of, a data unit that  
allows a recipient of the data unit to prove the source and integrity of the data unit and protect  
against forgery.  
15. Security implementation involves four complementary courses of action: prevention,  
detection, response, and recovery.  
**Please choose from the following concepts:**