Unit 33

Security Considerations

Omitted Parts:

33.11 Check Your Progress

1. A typical computerized environment constitutes three interdependent but separate components.
   (a) Software, hardware and data
   (b) Hardware, software and UPS
   (c) Software, modem and networking
   (d) Software, people ware and data
   (e) None of these
2. The risks broadly lead to:
   (a) Incorrect decision making leading to setback to business
   (b) Interruption in activities due to loss of data, hardware, software, people ware
   (c) Violation of privacy
   (d) Direct financial loss due to computer frauds
   (e) All of these
3. The phases of disaster recovery planning are:
   (a) Awareness
   (b) Preparation
   (c) Testing
   (d) Recovery
   (e) All of these
4. The consequences of errors in computerized systems are more serious than in manual systems because:
   (a) Computer systems process more data
   (b) Errors in computer systems are generated at high speed, and the cost to correct may be high
   (c) Users of computer systems perceive the computer outputs to be always correct
   (d) All of above
   (e) (a) and (c)
5. Compared to a manual system, in a computer system:
   (a) The methodologies for implementing controls change
   (b) Basic controls objectives change
   (c) Control objectives are more difficult to achieve
   (d) All of above
   (e) (a) and (b)
6. IS audit for the software used is carried out by CAATT. This type is known as:
   (a) The audit around the computer
   (b) The audit through the computer
   (c) The audit with the computer
   (d) All of above
   (e) None of these
7. Risk prone component(s) in computerized systems are:
   (a) Errors and omissions in data and software
   (b) Unauthorized disclosure of confidential information
   (c) Computer abuse and mis-utilisation of banks assets
   (d) Frauds
   (e) All of above
8. Effective control mechanism(s) in computerized environment are:
   (a) Preventive
   (b) Detective
   (c) Corrective
   (d) All of above
   (e) (a) and (c)
9. Objective of IS security is to ensure;
   (a) Confidentiality
   (b) Integrity
   (c) Availability
   (d) All of above
   (e) None of these

10. Audit trail is:

(a) A chronological record of all events occurring in a system is:
(b) Report submitted by auditors
(c) A collection of record generated by database administrator
(d) All of above
(e) None of these

33.12 ANSWERS TO 'CHECK YOUR PROGRESS'

1. (a), **2.** (e), **3.** (e), **4.** (d), **5.** (d), **6.** (c), **7.** (e), **8.** (d), **9.** (d), **10.** (a).

33.13 KEYWORDS

Data, Access Control Systems, Algorithm, Online, Password, Real time, Disaster.