

Learning Objectives:

After completing this course, you should be able to:

1. Identify requirements of the organizational security policies.
2. Recognize the three levels of security.
3. Recognize proper security safeguards.
4. Recognize the different lines of defense for a computer system.
5. Identify environmental considerations as they apply to computer security.
6. Recognize the components of a maintenance log.
7. Identify computer access controls for software and data files
8. Identify some of the most common hardware problems.
9. Identify how data integrity may be threatened.
10. Recognize some hardware security devices used to protect the computer system.
11. Identify top security related products in use.
12. Recognize different types of viruses and security threats.
13. Recognize the uses of firewall security systems.
14. Identify prerequisites for sensitive personnel positions.
15. Recognize the value of an employee performance evaluation system and components of a training system.
16. Identify security issues posed by terminated employees.
17. Recognize network tools used to implement security plans.
18. Identify the tools and techniques used by saboteurs.
19. Identify questions that policy makers should answer when designing a security system.
20. Recognize activities conducted as part of the risk analysis and management.
21. Recognize human factor threats for security.
22. Recognize the types of disruptions in computer processing.
23. Recognize components of a contingency plan.
24. Identify fire safety preventive plans.
25. Identify the scope of internal and external security auditing.
26. Recognize the audit trail to identify unusual activities.
27. Recognize control techniques.
28. Identify EDI security risks.
29. Recognize penalties of the US Computer Fraud and Abuse Act.
30. Identify major issues regarding computer crimes and privacy issues.
31. Identify new certificate programs in computer security.