مكتبة

"خُذْ وأعطِي"

الإلكترونية

جامعة آل البيت " كلية الإقتصاد "

مجموعة طلابية تسعى لتوفير كل ما يلزم طلاب
كلية إدارة المال والاعمال من مواد وشروحات واسئلة بصورة الكترونية

Chapter 5
MULTIPLE CHOICE

1. Perhaps the most striking fact about natural disasters in relation to AIS controls is that

   a) many companies in one locale can be seriously affected at one time by a disaster.
   b) losses are absolutely unpreventable.
   c) there are a large number of major disasters every year.
   d) disaster planning has largely been ignored in the literature.

2. There are four distinct types of threats to an AIS: 1) software errors and equipment malfunctions; 2) unintentional acts; 3) intentional acts; and 4) __________.

   a) computer fraud
   b) data transmission errors
   c) human carelessness
   d) natural and political disasters

3. Which AIS threat below would be classified an unintentional act?

   a) a power outage
   b) sabotage
   c) high winds
   d) a logic error

4. Which AIS threat below would be classified as a natural or political disaster?

   a) Accident
   b) Corruption
   c) Power outage
   d) Terrorist attack

5. Which AIS threat below would be classified a computer crime?

   a) Innocent error
   b) Operating system crash
   c) Sabotage
   d) Terrorist attack

6. Which AIS threat below would be classified as a software error or equipment malfunction?

   a) Earthquake
   b) Logic error
   c) Operating system crash
   d) Sabotage

7. An expert from the Information Systems Security Association estimates that the largest single source of security problems for systems is due to

   a) human errors and omissions.
   b) physical threats such as natural disasters.
   c) dishonest employees.
   d) fraud and embezzlement.

8. Fraud is any and all means a person uses to gain an unfair advantage over another person. Current and former employees of an organization are much more likely to

perpetrate fraud than external parties. The act by a person or group of persons resulting in materially misleading financial statements is called a(n)

a) misappropriation of assets.
b) employee fraud.
c) fraudulent financial reporting.
d) theft of assets.

9. Most fraud perpetrators are insiders because

a) insiders are more dishonest than outsiders.
b) insiders know more about the system and its weaknesses than outsiders.
c) outsiders are more likely to get caught than insiders.
d) insiders have more need for money than outsiders.

10. A majority of fraud perpetrators are

a) outsiders.
b) employees.
c) computer hackers.
d) vendors.

11. Misappropriation of assets can also be called

a) Computer fraud
b) Employee fraud
c) Fraudulent financial reporting
d) Management fraud

12. Intentional or reckless conduct that results in materially misleading financial statements is called

a) financial fraud.
b) misstatement fraud.
c) fraudulent financial reporting.
d) audit failure fraud.

13. The Treadway Commission studied 450 lawsuits against auditors and found that

a) misappropriation of assets was the reason for over one-half of the suits.
b) fraudulent financial reporting was the reason for over one-half of the suits.
c) white-collar criminals were responsible for only a fraction of the lawsuits.
d) only in a very few cases were financial statements falsified.

14. Researchers have compared the psychological and demographic characteristics of white-collar criminals, violent criminals, and the general public. They found that

a) few differences exist between white-collar criminals and the general public.
b) white-collar criminals eventually become violent criminals.
c) most white-collar criminals invest their illegal income rather than spend it.
d) most white-collar criminals are older and not technologically proficient.

15. Which of the factors listed below is *not* a common factor for fraud?

a) pressure to commit fraud
b) opportunity to commit fraud
c) desire to get even with the employer

d) rationalization for the crime

16. Reasons for committing a fraud include living beyond one's means, having heavy debts, or unusually high bills. Such a motivator for committing a fraud is commonly known as a

a) spark.
b) pressure.
c) flash-point.
d) catalyst.

17. Which of the following motivators would be a good indication of financial pressure that would contribute to employee fraud?

a) a big change for the better in an employee's lifestyle
b) an employee suddenly acquires lots of credit cards
c) inadequate internal controls
d) too close association with suppliers or customers

18. Which of the following emotions could cause an employee to feel pressured to defraud his employer?

a) a feeling of not being appreciated
b) failing to receive a deserved promotion
c) believing that their pay is too low relative to others around them
d) All of the above emotions could be sources of pressure.

19. There are three characteristics associated with most fraud. The characteristic that often takes more time and effort and leaves behind more evidence than other types of fraud is called

a) theft.
b) conversion.
c) concealment.
d) embezzlement.

20. In many cases of fraud, the __________ takes more time and effort than the __________ is worth.

a) concealment; theft
b) theft; concealment
c) conversion; theft
d) conversion; concealment

21. What is one common way to hide a theft?

a) by creating cash through the transfer of money between banks
b) by the conversion of stolen assets into cash
c) by stealing cash from customer A and then using customer B's balance to pay customer A's accounts receivable
d) by charging the stolen item to an expense account

22. In a __________ scheme, customer receipts are stolen and then subsequent payments by other customers are misapplied to cover the theft of the original receipts.

a) kiting

b) laundering
c) bogus expense
d) lapping

23. One fraudulent scheme covers up a theft by creating cash through the transfer of money between banks. This is known as

a) lapping.
b) misappropriation of assets.
c) kiting.
d) concealment.

24. Characteristics connected with fraud include pressures, opportunities, and rationalizations. Of these characteristics, which one often stems from a lack of internal controls within an organization?

a) pressures
b) opportunities
c) rationalizations
d) none of the above

25. Which situation below makes it easy for someone to commit a fraud?

a) the organization placing excessive trust in key employees
b) inadequate staffing within the organization
c) company policies within the organization are unclear
d) All of the above situations make it easy for someone to commit a fraud.

26. What is the most prevalent opportunity within most companies to commit fraud?

a) the failure to have any internal controls
b) the failure to enforce the system of internal controls
c) the failure to have the correct controls
d) the failure to realize that fraud could occur

27. Characteristics connected with fraud include pressures, opportunities, and rationalizations. Of these characteristics, which one relates to excuses that perpetrators have allowing them to justify their illegal behavior?

a) pressures
b) opportunities
c) rationalizations
d) none of the above

28. The US Justice Department defines computer fraud as

a) any crime in which a computer is used.
b) an illegal act in which knowledge of computer technology is essential.
c) any act in which cash is stolen using a computer.
d) an illegal act in which a computer is an integral part of the crime.

29. Computer fraud is often much more difficult to detect than other types of fraud because

a) perpetrators usually only steal very small amounts of money at a time, thus requiring a long period of time to have elapsed before they're discovered.
b) perpetrators can commit a fraud and leave little or no evidence.

c) most perpetrators invest their illegal income rather than spend it, thus concealing key evidence.
d) most computer criminals are older and are considered to be more cunning when committing such a fraud.

30. Why is computer fraud often more difficult to detect than other types of fraud?

a) Rarely is cash stolen in computer fraud.
b) The fraud may leave little or no evidence it ever happened.
c) Computers provide more opportunities for fraud.
d) Computer fraud perpetrators are just cleverer than other types of criminals.

31. Many fraud cases go unreported and unprosecuted for several reasons. Why is this the case?

a) Companies are reluctant to report computer crimes because a highly visible computer fraud is a public relations nightmare.
b) Such crimes are difficult, costly, and time-consuming to investigate and prosecute.
c) Law enforcement and the courts are often too busy with violent crimes that little time is left for fraud cases.
d) all of the above

32. Computer fraud can be analyzed using the traditional data processing model. According to this model, the simplest and most common fraud is __________ fraud.

a) input
b) processor
c) computer instructions
d) output

33. The simplest and most common way to commit a computer fraud is to

a) alter computer input.
b) alter computer output.
c) modify the processing.
d) corrupt the data base.

34. Computer fraud has been categorized into several different classifications. The classification of computer fraud where the perpetrator causes a company to pay for ordered goods, or to pay for goods never ordered is called

a) disbursement fraud.
b) inventory fraud.
c) payroll fraud.
d) cash receipts fraud.

35. In a disbursement fraud the company

a) pays too much for ordered goods.
b) pays for goods never received.
c) laps cash payments at the bank.
d) Both A and B are correct.

36. How can funds be stolen in payroll fraud?

a) by paying a fictitious or ghost employee
b) by increasing pay rates without permission
c) by keeping a real but terminated employee on the payroll

d) All of the above situations are possible.

37. Stealing a master list of customers and selling it to a competitor is an example of

a) data theft.
b) output theft.
c) disbursement fraud.
d) a trap door technique.

38. One computer fraud technique is known as data diddling. What is it?

a) gaining unauthorized access to and use of computer systems, usually by means of a personal computer and a telecommunications network
b) unauthorized copying of company data such as computer files
c) unauthorized access to a system by the perpetrator pretending to be an authorized user
d) changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data

39. What is a denial of service attack?

a) A denial of service attack occurs when the perpetrator sends hundreds of messages from randomly generated false addresses, overloading an Internet service provider's e-mail server.
b) A denial of service attack occurs when an e-mail message is sent through a re-mailer, who removes the message headers making the message anonymous, then resends the message to selected addresses.
c) A denial of service attack occurs when a cracker enters a system through an idle modem, captures the PC attached to the modem, and then gains access to the network to which it is connected.
d) A denial of service attack occurs when the perpetrator e-mails the same message to everyone on one or more Usenet newsgroups LISTSERV lists.

40. The unauthorized copying of company data is known as

a) Data leakage
b) Eavesdropping
c) Masquerading
d) Phishing

41. The unauthorized access to and use of computer systems

a) Hacking
b) Hijacking
c) Phreaking
d) Sniffing

42. Which of the following is the easiest method for a computer criminal to steal output without ever being on the premises?

a) dumpster diving
b) by use of a Trojan horse
c) using a telescope to peer at paper reports
d) electronic eavesdropping on computer monitors

43. Computer fraud perpetrators who use telephone lines to commit fraud and other illegal acts are typically called

a) hackers.
b) crackers.

c) phreakers.
d) jerks.

44. Gaining control of someone else's computer to carry out illicit activities without the user's knowledge

a) Hacking
b) Hijacking
c) Phreaking
d) Sniffing

45. Illegally obtaining and using confidential information about a person for economic gain

a) Eavesdropping
b) Identity theft
c) Packet sniffing
d) Piggybacking

46. Which of the following is not a method of identify theft

a) Scavenging
b) Phishing
c) Shoulder surfing
d) Phreaking

47. Which method of fraud is physical in its nature rather than electronic?

a) cracking
b) hacking
c) eavesdropping
d) scavenging

48. When a computer criminal gains access to a system by searching records or the trash of the target company, this is referred to as

a) data diddling.
b) dumpster diving.
c) eavesdropping.
d) piggybacking.

49. A part of a program that remains idle until some date or event occurs and then is activated to cause havoc in the system is a

a) trap door.
b) data diddle.
c) logic bomb.
d) virus.

50. The deceptive method by which a perpetrator gains access to the system by pretending to be an authorized user is called __________.

a) cracking.
b) masquerading.
c) hacking.
d) superzapping.

51. Tapping into a communications line and then entering the system by accompanying a legitimate user without their knowledge is called

    a) superzapping.
    b) data leakage.
    c) hacking.
    d) piggybacking.

52. A fraud technique that slices off tiny amounts from many projects is called the __________ technique.

    a) Trojan horse
    b) round down
    c) salami
    d) trap door

53. Spyware is

    a) Software that tells the user if anyone is spying on his computer
    b) Software that monitors whether spies are looking at the computer
    c) Software that monitors computing habits and sends the data it gathers to someone else
    d) None of the above

54. The unauthorized use of special system programs to bypass regular system controls and perform illegal act is called

    a) a Trojan horse.
    b) a trap door.
    c) the salami technique.
    d) superzapping.

55. Computer fraud perpetrators have developed many methods to commit their acts. One way is to modify programs during systems development allowing access into the system that bypasses normal system controls. This is known as

    a) a Trojan horse.
    b) a trap door.
    c) the salami technique.
    d) superzapping.

56. A fraud technique that allows the hacker to bypass normal system controls and enter a secured system is called

    a) superzapping.
    b) data diddling.
    c) using a trap door.
    d) piggybacking.

57. A set of unauthorized computer instructions in an otherwise properly functioning program

    a) Logic bomb
    b) Spyware
    c) Trap door
    d) Trojan horse

58. A __________ is similar to a __________, except that it is a program rather than a code segment hidden in a host program.

   a) worm; virus
   b) Trojan horse; worm
   c) worm; Trojan horse
   d) virus; worm

59. Which type of antivirus program is most effective in spotting an infection soon after it starts?

   a) a virus protection program
   b) a virus identification program
   c) a virus detection program
   d) none of the above

60. How can an organization reduce fraud losses?

   a) encrypt data and programs
   b) use forensic accountants
   c) maintain adequate insurance
   d) require vacations and rotate duties

SHORT ANSWER

61. Define fraud.

62. What are the two kinds of fraud in business?

63. What are the actions recommended by the Treadway Commission to reduce the possibility of fraudulent financial reporting?

64. What are the three common things that happen in a fraud?

65. What techniques are used to conceal theft by fraud?

66. What is a computer fraud?

67. Why is computer fraud on the rise?

68. How can a system be protected from viruses?

69. Discuss antivirus software programs.

70. How does a company make fraud less likely to occur?

71. How can companies reduce losses from fraud?

ESSAY

72. What are some of the distinguishing characteristics of fraud perpetrators?

73. What is the difference between a worm and a virus?

74. What are some of the computer fraud techniques used by perpetrators?

75. Why do fraudulent acts often go unreported and are therefore not prosecuted?

ANSWER KEY

1) A
2) D
3) D
4) D
5) C
6) C
7) A
8) C
9) B
10) B
11) B
12) C
13) B
14) A
15) C
16) B
17) A
18) D
19) C
20) A
21) D
22) D
23) C
24) B
25) D
26) B
27) C
28) B
29) B
30) B
31) D
32) A
33) A
34) A
35) D
36) D
37) A
38) D

39) A
40) A
41) A
42) D
43) C
44) B
45) B
46) D
47) D
48) B
49) C
50) B
51) D
52) C
53) C
54) D
55) B
56) C
57) D
58) A
59) D
60) C
61) Fraud is any means a person uses to gain an unfair advantage over another. Fraud usually involves the misrepresentation of facts about a situation and the reliance on that misrepresentation by the victim. Frauds are often called "cons" because they involve a violation of trust or confidence.
62) Employee Fraud is a misappropriation of assets, or theft, by a person or group for personal financial gain. Fraudulent financial reporting is intentional or reckless conduct that results in materially misleading financial statements.
63) Establish an organizational environment that contributes to the integrity of the financial reporting process. Identify and understand the factors that lead to fraudulent financial reporting. Assess the risk of fraudulent financial reporting within the company. Design and implement controls to provide reasonable assurance that the fraudulent financial reporting is prevented
64) Theft of an asset. Conversion to cash (if not already cash). Concealment of the crime
65) Some techniques used to conceal theft by fraud are charging stolen assets to an expense account, lapping or misapplying cash payments from customers and stealing part of the receipts, kiting or creating fictitious bank balances by shuttling monies between bank accounts, and playing the bank float, then stealing some of the cash.
66) Computer fraud is any illegal act for which knowledge of computer technology is essential for its perpetration, investigation, or prosecution.
67) Not everyone agrees on what constitutes computer fraud and some people may commit computer fraud unwittingly and not be aware of it. Many computer frauds go undetected. The belief that "it just can't happen to us". Most networks have a low level of security. Many Internet sites provide guidance on how to commit computer crimes. Law enforcement is unable to keep up with the number of computer frauds. Most frauds are not reported. The total dollar value of losses is difficult to calculate.
68) Install reliable antivirus software that scans for, identifies, and isolates or destroys viruses. Use caution when copying files on to your diskettes from unknown machines. Ensure the latest versions of the antivirus program available is used. Scan all incoming emails for viruses at the server level. All software should be certified as virus-free before loading it into the system. If you use jump drives, diskettes, or CDs, do not put them in unfamiliar machines as they may become infected. Obtain software and diskettes only from known and trusted sources. Use caution when using or purchasing software or diskettes from unknown sources. Deal with trusted software retailers. Ask whether the software you are purchasing comes with electronic techniques that makes tampering evident. Check new software on an isolated machine with virus detection software before installing on the system. Cold boot to clear and reset the system. When necessary,

"cold boot" the machine from a write-protected diskette. Have two backups of all files. Restrict the use of public bulletin boards.

69) There are three types of antivirus software programs. Virus protection programs are designed to remain in computer memory and search for viruses trying to infiltrate the system. When an infection attempt is detected, the software freezes the system and flashes a message to the user. Virus detection programs spot an infection soon after it starts. Virus identification programs scan all executable programs to find and remove all known viruses from the system.

70) A company can decrease fraud by: good hiring and firing practices; good management of unhappy employees; training in fraud awareness; manage and track computer licenses; implement signed confidentiality agreements; maintain visible security; educate the workforce in ethics and the penalties for illegal acts.

71) Maintain adequate insurance. Keep a current backup copy of all program and data files in a secure off-site location. Develop a contingency plan for fraud occurrences and other disasters that might occur. Use special software designed to monitor system activity and help companies recover from frauds and malicious actions.

72) Some distinguishing characteristics of fraud perpetrators are: they tend to spend their illegal income to support their lifestyle; once they begin it becomes harder to stop and they become bolder as each incident happens; once they start to rely on the ill-gotten gains, they become more greedy and sometimes careless and overconfident. In the case of computer criminals, they are often young and have substantial computer knowledge. About two-thirds are men and likely to be an employee of the firm from which they steal. Many are unhappy or disgruntled with their employer because they feel unappreciated and underpaid. Most have no previous criminal record.

73) A computer virus is a segment of executable code that attaches itself to computer software. A virus has two phases: it replicates itself and spreads to other systems or files, and in the attack phase, the virus carries out its mission to destroy files or the system itself. A worm is similar to a virus, except that it is a program rather than a code segment hidden in a host program. A worm can reside in e-mail attachments, which when opened or activated can damage a user's system. Worms can also reproduce themselves by mailing themselves to the addresses found in the recipient's mailing list. Worms do not have long lives, but their lives can be very destructive nonetheless.

74) Various computer fraud techniques include: Trojan horse - unauthorized code hidden in a legitimate program. Round-down technique - rounded off amounts from calculations and the fraction deposited in perpetrator's account. Salami technique - small amounts sliced off and stolen from many projects over a period of time. Trap door - bypass of normal system controls. Superzapping - use of a special program to bypass regular controls. Software piracy - unauthorized copying of software, probably the most committed computer crime. Data diddling - changing data in an unauthorized way. Data leakage - unauthorized copying of data files. Piggybacking - latching onto a legitimate user in data communications. Masquerading or Impersonation - the perpetrator gains access to the system by pretending to be an authorized user. Social engineering - a perpetrator tricks an employee into giving him the information he needs to get into the system. Logic bomb - idle until some event or time triggers it. Hacking - unauthorized access and use of a computer system. Scavenging - gaining access to confidential data by searching corporate records in dumpsters or computer storage. Eavesdropping - observation of private communications by wiretapping or other surveillance techniques. E-mail threats - threatening legal action and asking for money via e-mail. E-mail forgery - removing message headers, using such anonymous e-mail for criminal activity. Denial of service attack - sending hundreds of e-mail messages from false addresses until the attacked server shuts down. Internet terrorism - crackers using the Internet to disrupt electronic commerce and communication lines. Internet misinformation - using the Internet to spread false or misleading information. War dialing - searching for idle modem by dialing thousands of telephones and intruding systems through idle modems. Spamming - e-mailing the same message to everyone on one or more Usenet groups.

75) Most fraud cases go unreported and are not prosecuted for several reasons. Many cases of computer fraud are as yet still undetected. As new technology and methods become available to organizations, prior undetected fraud may be revealed in the future. A second reason is that companies are reluctant to report computer fraud and illegal acts simply because of bad publicity--a highly visible case can undermine consumer confidence in an organization such as a financial

institution. Also, the fact that a fraud has occurred may indeed encourage others to attempt to commit further acts against the organization. It would seem that unreported fraud creates a false sense of security, as people think systems are more secure than they are in reality. Another reason for not reporting fraudulent acts is the fact that the court system and law enforcement is busy with violent crimes and criminals in its system. There is little time left to go after a crime where no physical harm is present. Also, the court system tends to treat teen hacking and cracking as "acts of childhood" rather than as serious crimes--this leads to many plea bargains when a computer fraud is brought to trial. Another reason is that a computer fraud case is difficult, costly, and time-consuming to investigate and prosecute. Before 1986 no federal law existed governing computer fraud. Law enforcement officials, lawyers, and judges generally lack the computer skills necessary to properly evaluate, investigate, and prosecute computer crimes. Sadly, when all is said and done a successful prosecution and conviction of computer fraud results in a very light sentence. All of these factors contribute to the underreporting and lack of prosecution of computer fraud crimes. Not everyone agrees on what constitutes computer fraud:

- Many networks have a low level of security
- Many Internet pages give instruction on how to carry out computer crimes
- Law enforcement has difficulty keep up with the growing number of computer frauds
- The total dollar value of losses from computer fraud is difficult to estimate.