KABARAK UNIVERSITY

UNIVERSITY EXAMINATIONS
2010/2011 ACADEMIC YEAR

FOR THE DEGREE OF BACHELOR OF BUSINESS MANAGEMENT & INFORMATION TECHNOLOGY

COURSE CODE: BMIT 416

COURSE TITLE: IT SECURITY ETHICS AND AUDIT

STREAM: Y4S1

DAY: FRIDAY

TIME: 9.00 – 12.00 P.M

DATE: 10/12/2010

INSTRUCTIONS:

- Answer all the questions in part one and any three questions in part two

PLEASE TURNOVER

PART ONE
QUESTION ONE (40 MARKS)

a. In information security what does the acronym CIA stand for? (3 marks)
b. In biometrics describe the;

i. Enrolment process (2 marks)
ii. Authentication process (2 marks)

c. Give two disadvantages of Biometric authentication methods. (2 marks)
d. Give two differences between an encryption and a hashing. (4 marks)
e, What is meant by two factor authentication? (1 mark)
f. Briefly describe an auto replay attack. (2 marks)
g. Describe two methods that can be used to protect against an auto replay attack. (4 marks)
h. Cryptographic systems usually work in a series of four stages; briefly describe them. (6 marks)
i. Give one example of a cryptographic system (1 mark)
j. Describe the public key encryption method (3 marks)
k. Name two public key encryption algorithms (2 marks)
l. Give two methods that can be used to protect symmetric keys used in a communication session from being cracked (4 marks)
m. Two communicating devices A and B need to communicate securely. Device A uses a cryptographic system that uses DES while device B uses 3DES. Describe how the two devices will encrypt the information sent between them. (4 marks)

PART TWO
QUESTION TWO (20 MARKS)

a. What is
i. A Trojan horse (1 mark)
ii. Spyware (1 mark)
b. Describe how a file integrity checker can be used to provide security for a server. (3 marks)
c. How do the following actions help in IT security?
i. Installing operating system patches (2 marks)
ii. Turning off unnecessary services running on a computer (2 marks)
d. Describe three reasons why it is important to implement application security. (3 marks)
e. Describe four actions that you can take to secure an application. (4 marks)
f. Describe two types of denial of service attacks (4 marks)

QUESTION THREE (20 MARKS)

a. Briefly describe the four different categories of security incidents (4 marks)
b. What is the disadvantage of a software agent on a monitored device in distributed intrusion detection system doing analysis and alarm generation? (2 marks)
c. Describe two ways in which an agent transfers log files to the manager in a distributed intrusion detection system. Give one advantage of each method. (4 marks)
d. Why is it important to have legal personnel as part of an organizations emergency response team? (1 mark)
e. How does backup fit in the intrusion response process? (1 mark)
f. If you were managing backup for an organization describe four actions that you would include in your backup plan? (4 marks)
g. Describe two types of backup facilities that can be used in a disaster recovery plan. (4 marks)

QUESTION FOUR (20 MARKS)

a. One step involved in risk analysis is asset classification. Describe two methods that can be used to classify assets in an organization. (4 marks)
b. Describe three ways that an organization can respond to risks. (6 marks)
c. The following table contains information about a particular asset in an organization.

	Threat A	Threat B	Threat C	Threat D	Threat E	Threat F
Cost if attack succeeds (in Kenya shillings)	100000	1000000	40000	10000	500000	350000
Probability of occurrence (as a percentage)	20	5	50	70	10	90
Cost of protection against threat (in Kenya shillings)	5000	60000	30000	1000	100000	200000

Perform risk analysis calculation to determine which protection are economically worthwhile (6 marks)

d. Name two security functions that an organization can outsource to a managed security service provider. (2 marks)
e. Give two advantages of outsourcing some security functions to managed security service providers. (2 marks)

QUESTION FIVE (20 MARKS)

a. Describe three general principles that are used as guidelines in security architecture design. (6 marks)

b. Why do some organizations hire hackers as IT security personnel? (2 marks)

c. Users are an important component in IT security, and one way of ensuring this is by training them. Describe three important areas that users should be trained in order to make them full time partners in security. (3 marks)

d. Give four reasons why some companies monitor their employees. (4 marks)

e. Give two ways in which companies can monitor their employees, (2 marks)

f. What is a computer and internet use policy? (3 marks)