



JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR SCIENCE

EDUCATION SCIENCE/ARTS

4th YEAR 1st SEMESTER ACADEMIC YEAR MAIN CAMPUS

MAIN CAMPUS SB

COURSE CODE: SCS 436

COURSE TITLE: INTERNAL CONTROLS AND SECURITY ISSUES

EXAM VENUE: HALL 1

STREAM: BED ARTS/SNE

DATE: 27/04/16

EXAM SESSION: 2.00 – 4.00 pm

TIME: 2.00 HOURS

INSTRUCTIONS:

- 1. Answer Question 1 (Compulsory) and ANY other two questions.**
- 2. Candidates are advised not to write on the question paper.**
- 3. Candidates must hand in their answer booklets to the invigilator while in the examination room.**

QUESTIONS ONE 30 MARKS}.

- a) What has become more important because of the increased use of computers, the internet and WWW.
- i. Natural Disasters
 - ii. Hardware Malfunctions
 - iii. Data integrity and data security
 - iv. Malicious deletions.
- b) Accurate and complete data enters the system for processing and remains accurate thereafter, is said to have:
- i. Integrity
 - ii. Security
 - iii. Viruses
 - iv. Accidental deletion.
- c) What is the difference between Data Integrity and Data Security?
- i. Limiting physical access to computer systems; assigning passwords to users
 - ii. Consistent, accurate and reliable data; protection of data from unauthorized access.
 - iii. Encryption; Audit trails
 - iv. Distributing work to preserve integrity; installing system passwords
- d) Control in design of an information system is used to
- i. inspect the system and check that it is built as per specifications
 - ii. protect data from accidental or intentional loss
 - iii. ensure that the system processes data as it was designed to and that the results are reliable
 - iv. ensure privacy of data processed by it
- e) Controls are necessary in information systems as
- (i) massive amounts of data are processed and human errors are expected in data entry
 - (ii) accidental errors can lead to loss of money and credibility in a system
 - (iii) to protect the system from virus attack
 - (iv) data may be lost due to disk crashes

a. i and ii

- b. i and iii
- c. i and iv
- d. ii and iii

f) The major objectives of control are

- i. guard against frauds in data entry/processing
- ii. check clerical handling of data before it enters a computer
- iii. to provide a method to trace the steps and find where error has occurred
- iv. automatically correct errors in data entry/processing

- a. i, ii and iv
- b. i, ii, iii and iv
- c. i, ii and iii
- d. i and iii

g) Audit in the design of information system is used to

- a. inspect the system and check that it is built as per specifications
- b. protect data from accidental or intentional loss
- c. ensure that the system processes data as it was designed to and that the results are reliable
- d. ensure privacy of data processed by it

h) Auditing of information systems is primarily required to ensure the

- (i) all input records are correct and are included in processing
- (ii) the system has ample protection against frauds
- (iii) the processing performance is reliable
- (iv) the system is developed at low cost

- a. i and ii
- b. iii and iv
- c. ii and iii
- d. i, ii and iii

i) An audit trail is established in a system to

- a. detect errors in a system

- b. enable auditing of a system
- c. localize the source of an error in a system
- d. trail a program

j) Some audit and control procedures in a system

(i) detect and correct errors in programs

(ii) selectively print records in a system which meet certain criteria

(iii) examine credit and debit balances in an accounting system and check if they balance

(iv) provide a facility to trace a variable value through processing steps and print intermediate values when required

- a. i and ii
- b. ii and iii
- c. i, ii, iii
- d. ii, iii, iv

k) Security in the design of information system is used to

- a. inspect the system and check that it is built as per the specifications
- b. protect data and programs from accidental or intentional loss
- c. ensure that the system processes data as it was designed to and that the results are reliable
- d. ensure privacy of data processed by it

l) By security of an information system we mean protecting

(i) data from accidental or intentional damage or loss

(ii) programs from accidental or intentional corruption or loss

(iii) programs and data from unauthorized disclosure or change

(iv) individual private data from disclosure

- a. i and ii
- b. i and iii

c. i, ii, iii

d. i, ii, iii, iv

m) Some security measures commonly used are

(i) data encryption

(ii) logging of all accesses to an information system and recording changes made (if any)

(iii) data compression

(iv) copying of files

a. ii and iii

b. i and iii

c. i and ii

d. ii and iv

n) To protect a system from viruses one should

(i) not allow unauthorized use of floppy disks

(ii) scan viruses in files received via a network or floppies

(iii) isolate a system from networks

(iv) install a roll-back recovery program in the system

a. i and iii

b. i and ii

c. ii and iv

d. i, iii, iv

o) A firewall is used in a system connected to a wide area network to

a. prevent spread of fire in the network

b. prevent unauthorized access by hackers

c. to scan for viruses in files

d. to extinguish fire spreading via network cables

QUESTION 2 [20 MARKS]

- a) Discuss THREE objectives of Internal Controls { 6 marks }
- b) You have just acquired a job at MALOMALO Company Ltd (an IT outsourcing Company) as the Chief Security Officer. Your main task is to give the management high level of Assurance on the security of their systems and processes within the company. Your first assignment would be to establish security requirements for MALOMALO company. Explain how you would go about this task { 14 marks }

QUESTION 3 [20 MARKS]

- a) Discuss the risk management process { 8 marks }
- b) Define a Computer Crime { 2 marks }
- c) Explain the conditions that necessitate fraud to occur within an organization { 6 marks }
- d) Giving example, discuss any 4 classifications of computer fraud { 4 marks }

QUESTION 4 [20 MARKS]

- a) Discuss the five elements of the Internal Control Environment using any organization as a reference point { 10 marks }
- b) Using an example , explain the term Segregation of Duties (SOD) { 2 marks }
- c) Explain the following aspects of security { 2 marks Each }
- i. Physical security
 - ii. Intrusion detection
 - iii. Logical security
 - iv. Awareness training

QUESTION 5 [20 MARKS]

a) The following is a categorization of controls. Identify the type of control provided by each of the controls in each category { 8 marks }

Physical Controls	Preventive	Detective	Corrective	Deterrent	Recovery	Compensative
<i>Fences</i>						
<i>Lock</i>						
<i>Badge System</i>						
<i>Manstrap Doors</i>						
<i>Offsite Facility</i>						
Administrative controls	Preventive	Detective	Corrective	Deterrent	Recovery	Compensative
<i>Security Policy</i>						
<i>Separation of Duties</i>						
<i>Job Rotation</i>						
<i>Information Classification</i>						
<i>Personnel procedures</i>						

b) Differentiate between Financial Audits and Information Systems Audits { 4 marks }

c) Describe the information Systems Audit Process { 8 marks }