KENYA METHODIST UNIVERSITY

END OF 1ST TRIMESTER 2010 EXAMINATIONS

FACULTY	**:**	**COMPUTING AND INFORMATICS**
DEPARTMENT	**:**	**COMPUTER INFORMATION SYSTEMS**
UNIT CODE	**:**	**CISY 438**
UNIT TITLE	**:**	**ADVANCED INFORMATION SYSTEMS SECURITY**
TIME	**:**	**2 HOURS**

Instructions:

- *Answer question 1 and any other 2 questions.*

Question 1 (30 marks)

a) Differentiate between; (6 mks)
   i) IDS and firewall
   ii) IT security and information security
   iii) Security model and security policy

b) What is information systems auditing? Why is it necessary? (5 mks)

c) Security design is a must when designing software; give any four software security principles. (4 mks)

d) Giving advantages and disadvantages of each compare between qualitative and quantitative approaches of risk assessment. (6 mks)

e) What are some of the key elements of the business process evaluation? (4 mks)

f) What are the pillars of IT service delivery? Explain. (3 mks)

g) What is SLA? Why do we need it in IT systems service delivery? (2 mks)

Question 2 (20 marks)

a) Why do companies need a security policy? (2 mks)

b) There are many types of threat agents, give and explain the agents, several types of vulnerabilities and the resulting specific threats. (8 mks)

c) There are six steps that help when you are responding to a security incident quickly and efficiently. Give and explain each step. (6 mks)

d) Give and explain four ways which you respond to a risk. (4 mks)

Question 3 (20 marks)

a) Each of the access controls categories – administrative, physical and technical, work at different levels, each at a different level of granularity and perform different functionalities based on the type. Explain each level. (9 mks)

b) Use a risk matrix to evaluate threats and countermeasures. (6 mks)

c) What is IT governance? How do you establish it? (5 mks)

Question 4 (20 marks)

a) Name and explain any three security models. (6 mks)

b) There are some guidelines to compliance investigations. State and explain any four. (4 mks)

c) There are three types of cryptographic algorithms. State and explain the working principle of each. (6 mks)

d) What factors would you consider when developing an information security program? (4 mks)