SOUTH EASTERN KENYA UNIVERSITY

UNIVERSITY EXAMINATIONS 2015/2016

MAY-AUGUST 2016 (PRACTICUM) SEMESTER EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE (INFORMATION SYSTEMS)

SCI508: INFORMATION SYSTEM SECURITY CONTROL AND AUDIT

DATE: 10TH AUGUST, 2016 **TIME: 2.00 – 5.00 PM**

INSTRUCTIONS TO CANDIDATES

a) **Answer ALL questions from section A(Compulsory)**

b) **Answer ANY TWO questions from section B**

SECTION A (30 Marks) - Compulsory

Question One

a. Define the following terms:
   i. Audit Risk;
   ii. Risk-based Audit;
   iii. Materiality;
   iv. Substantive Testing. (8 marks)

b. Describe six basic outcomes of effective security governance. (12 marks)

c. An IS auditor is planning to review the security of a financial application for a large company with several locations worldwide. The application system is made up of a web interface, a business logic layer and a database layer.
   The application is accesses locally through a LAN and remotely through the Internet via a virtual private network (vpn) connection.
   Required
   i. Suggest the appropriate CAATs tool the auditor should use to test security configuration settings for the entire application system. Justify your answer. (5 marks)
   ii. Given that the application is accessed through the Internet, explain how the auditor should determine whether to perform a detailed review of the firewall rules and vpn configuration settings. (5 marks)

SECTION B (40 Marks): ANSWER ANY TWO QUESTIONS

Question Two

a. Discuss Information Systems Risk analysis. (10 marks)
b. Discuss the Business Model for Information Security. (10 marks)

Question Three

a. Explain FIVE Information Security Strategy Objectives. (10 marks)
b. Describe THREE control classifications, their functions and usages. (10 marks)

Question Four

a. Describe FIVE common pitfalls to avoid when developing an information security strategy. (10 marks)
b. Discuss FIVE audit classifications. (10 Marks)

END.