JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE MASTER OF IT SECURITY AND AUDIT

1st YEAR 2nd SEMESTER 2018/2019 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: IIT 5124

COURSE TITLE: RISK MANAGEMENT

EXAM VENUE: STREAM:

DATE: EXAM SESSION:

TIME: 2.00 HOURS

INSTRUCTIONS:

1. **Answer Question 1 (Compulsory) and ANY other three 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**

QUESTION ONE 20 MARKS

a) Describe the following terms as used in IT Security and Risk Management
   i. Risk Leverage **(2 Marks)**
   ii. Vulnerability **(2 Marks)**
   iii. Computer Security **(2 Marks)**
   iv. Eavesdropping **(2 Marks)**
   v. Spoofing **(2 Marks)**
   vi. Repudiation **(2 Marks)**
   vii. Exploits **(2 Marks)**
   viii. Encryption **(2 Marks)**

b) Availability attacks, sometimes called denial-of-service or DOS attacks, are much more significant in networks than in other contexts. There are many accidental and malicious threats to availability or continued service. In what ways is denial of service (lack of availability for authorized users) a vulnerability to users of single-user personal computers? **(4 Marks)**

QUESTION TWO 20 MARKS

a) List three factors that should be considered when developing a security plan. **(3 Marks)**
b) Explain the risk management process **(6 Marks)**
c) In order to assess the level of risk, likelihood and the impact of incidental occurrences should be estimated. This estimation can be based on experience, standards, experiments, expert advice, etc. You are required to describe Risk analysis or assessment approach in terms of quantitative, semi quantitative and qualitative. **(6 Marks)**
d) Describe FIVE principles of information security **(5 Marks)**

QUESTION THREE 20 MARKS

a) Cite a reason why an organization might want two or more firewalls on a single network. **(2 Marks)**
b) We distinguish a risk from other project events by looking for three things. Describe these three things that are used in distinguishing a risk from any other project event. **(6 Marks)**
c) Risk analysis is a well-known planning tool, used often by System auditors, accountants, and managers. Describe three good reasons to perform a risk analysis in preparation for creating a security plan. **(6 Marks)**
d) Risk is inevitable in life. You are required to discuss THREE strategies that can be used in dealing with the risks. **(6 Marks)**

QUESTION FOUR 20 MARKS

a) Describe the term Risk Assessment **(2 Marks)**
b) Describe a risk management plan **(2 Marks)**
c) Describe eight steps involved in the methodology of risk management according to Sp800-30 NIST (National Institute of Standards and Technology) Risk Management Guide for Information Technology systems. **(16 Marks)**

QUESTION FIVE 20 MARKS

a) What is a Business Continuity Plan? **(1 Mark)**
b) Describe FOUR situations in which a business continuity plan would be helpful. **(8 Marks)**
c) The key to coping with Information System disasters is advance planning and preparation, identifying activities that will keep a business viable when the computing technology is disabled. Outline three steps in business continuity planning. **(6 Marks)**
d) Investigate your university's or employer's security plan to determine whether its security requirements meet all the conditions we studied during this course. Outline atleast FIVE Network security threats **(5 Marks)**