JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTERS OF IT SECURITY & AUDIT

2ND YEAR 1ST SEMESTER 2022/2023 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: IIT 5216

COURSE TITLE: DISASTER RECOVERY AND BUSINESS CONTINUTY

EXAM VENUE: KISUMU CAMPUS **STREAM: IT SECURITY & AUDIT**

DATE: **EXAM SESSION: 2 HOURS**

TIME:

INSTRUCTIONS

1. **Answer ANY 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 1 [20 marks]

a) Using a diagram describe what contingency planning is and how it relates to incident response planning, disaster recovery planning, and business continuity plans. **(10 marks)**

b) ISO/IEC 24762:2008 provides guidelines on the provision of information and communications technology disaster recovery (ICT DR) services. It serves to demonstrate that the certified professional holds defined competencies based on best practices. Briefly discuss the 10 clauses of this standard. **(10 marks)**

Question 2 [20 marks]

The attacks of September 11, 2001 provided no warning. Two companies, Barclays Capital, Putnam Investments and Tulane University learned some hard lessons that day. Wall Street and its financial institutions were reminded about the importance of a good disaster recovery plan.

a) Briefly discuss how each was affected by the disasters
   i) Barclays Capital. **(5 marks)**
   ii) Tulane University. **(5 marks)**

b) Briefly discuss any ten lessons learnt for across the three organizations. **(10 marks)**

Question 3 [20 marks]

Threat assessment is the foundation for discovery of threats and their possible levels of impact. It helps to It helps define the different levels of impact and to develop a risk mitigation plan

a) Identify five possible threats that an IT organization is likely to face. **(5 marks)**
b) Briefly discuss the three basic recovery phases in disaster recovery. **(10 marks)**
c) What kind of strategies would you recommend in disaster recovery? **(5 marks)**

Question 4 [20 marks]

In order to mitigate cyber threats and foster a safer Kenyan cyberspace, the Kenyan government established the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), which is a multi-agency collaboration framework that is responsible for the national coordination of cyber security as well as Kenya's national point of contact on cyber security matters. This in accordance with the provisions of the Kenya Information and Communications Act 1998 (as amended), which mandates the Communications Authority of Kenya with developing a national framework for the investigation and prosecution of cybercrimes.

a) Briefly discuss any five functions of KE-CIRT/CC. **(10 marks)**
b) Discuss four essential services provided by KE-CIRT/CC. **(10 marks)**

Question 5 [20 marks]

The paper "Recovering from Database Recovery: Case Studies and the Lessons They Teach" by Mary J. Hoferek, Member, IEEE, and Susan C. Wilson and presented at the Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY 20-22 June 2007, was a wakeup call to IT managers about the importance of developing an effective Disaster Recovery Plan.

a) Describe and evaluate the organizations practices that contributed to the failure or success in safeguarding their organization's information assets. **(10 marks)**
b) Develop a Disaster Recovery Plan (DRP) for one of the selected organizations. **(10 marks)**