JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS
UNIVERSITY EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN HEALTH INFORMATICS
1ST YEAR 2ND SEMESTER 2018/ 2019 ACADEMIC YEAR
KISUMU CAMPUS

COURSE CODE: **IIT 6115**

COURSE TITLE: **ORGANIZATIONS CORPORATE COMPUTER AND NETWORK SECURITY**

EXAM VENUE: **KISUMU CAMPUS**

DATE: 14/08/19 **STREAM: PhD IT SECURITY AND AUDIT**

TIME: 3 HOURS **EXAM SESSION: 2.00 – 5.00PM**

INSTRUCTIONS:

1. **Answer any three (3) 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) When tasked with the responsibility to protect the resources in an organization's corporate information system infrastructure, you must first and foremost carefully define the scope of you work.

   i. Using documented knowledge from theory and practice, clearly discuss four factors you would consider in defining the scope of this task. (4 marks)

   ii. Identify and clearly discuss four internal and/ or external documents that would help you define the scope in (i) above. For each document, state its source and how it would help you do the work. (4 marks)

b) According to Horne et al. (2016), the theories or knowledge within any discipline are explained based on the following four ideas namely domain, ontology, epistemology and socio-political factors.

   Required

   Explain how proper understanding and contextualization of each of these concepts would provide relevance to a scholar intending to create new knowledge in ICT security that would be useful to a practitioner in the said field. (12 marks)

QUESTION TWO (20 MARKS)

a) Cyber and information warfare is a very critical concept in the field of ICT security and therefore deserves to be given necessary attention by all information technology security scholars and practitioners alike. In the light of the above statement, answer the following questions:

   i. From a scholar's perspective, discuss the documented paradigm shift in cyber warfare over time. (4 marks)

   ii. In your own opining, discuss the likely motivations behind this shift in (i) above. (3.5 marks)

   iii. Explain why an ICT security practitioner needs to understand this paradigm shift and how it would affect his work. (2 marks)

b) Labucki (1995) postulated 7 categories of information warfare. By and large, these categories are still very applicable in ICT security today. Taking cognizance of this statement, answer the following questions.

   i. Outline each of the seven (7) categories. (3.5 marks)

   ii. Discuss how each of the seven (7) would influence your decision and action as an information system security practitioner or advisor. (7 marks)

QUESTION THREE (20 MARKS)

The government of Kenya established the ICT Authority with the mandate to set and enforce ICT standards and guidelines across all aspects of information and communication technology including systems, infrastructure, processes, human resources and technology for the public service. The authority in its work established that the computer network is the infrastructure that enables all the other ICT services to integrate, synchronized and operate. Therefore authority identified nine standards which fall in six domain areas.

Required:

i. Explain the nine standards and the domains in which they fall (9 marks)

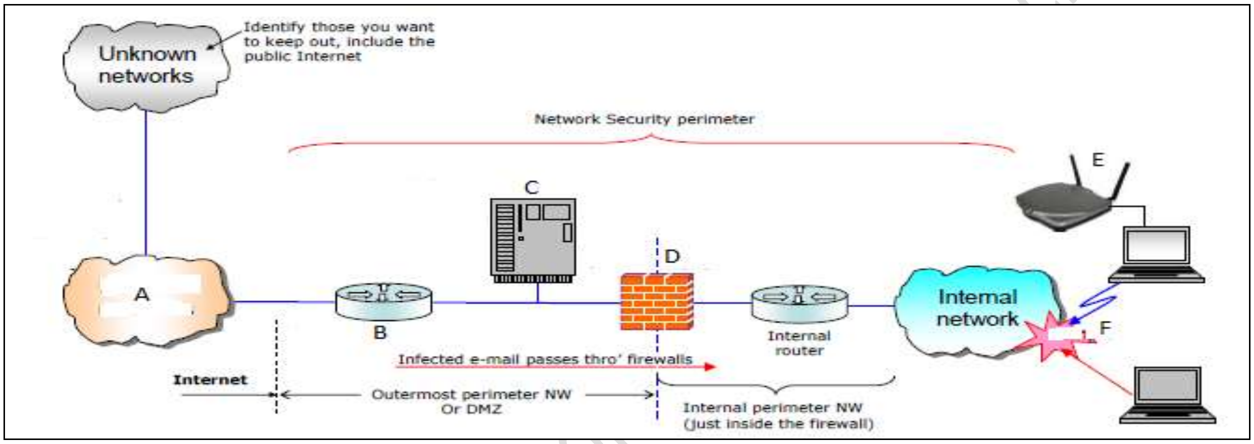
ii. Discuss how the introduction of these standards would affect.

a) The role of ICT experts including ICT security experts. (4 marks)

b) The national government departments and corporations as well as county government in managing their ICT infrastructure. (7 marks)

QUESTION FOUR (20 MARKS)

The figure below represents computer network of an organization. Study it carefully then answer the questions that follow.


Unknown networks
Identify those you want to keep out, include the public Internet
Network Security perimeter
A
B
C
D
E
F
Internal router
Internal network
Infected e-mail passes thro' firewalls
Internet
Outermost perimeter NW Or DMZ
Internal perimeter NW (Just inside the firewall)

Required:

i. State the parts labeled A, B, C, D, E and F. (3 marks)

ii. Explain at least two (2) roles of part B (4 marks)

iii. State any three network services that can be found in part C. (3 marks)

iv. Explain the problem at the part labeled F (2 marks)

v. Explain the probable cause of the problem in (iv) above (2 marks)

vi. Explain the main function of the part labeled D. (2 marks)

vii. Critically analyze this network infrastructure design, pointing out its key weakness and recommend how it can be improved. (4 marks)

QUESTION FIVE (20 MARKS)

As an information system security expert, you are supposed know all the information assets in your organization that you are required to protect. One important standard for enterprise information security management is the ISO/IEC 27001:2013 ISMS standard. It defines asset categories into seven.

Required

i. Identify and explain all the seven asset categories. (7 marks)

ii. Discuss five (5) benefits an organization can derive from getting ISO/IEC 27001:2013 certified. (5 marks)

iii. Critically analyses the strengths and weaknesses of this standard with regards to protecting the information assets in an organization operating in Kenya. (8 marks)