MURANG'A UNIVERSITY OF TECHNOLOGY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION TECHNOLOGY

UNIVERSITY POSTGRADUATE EXAMINATION

2018/2019 ACADEMIC YEAR

FIRST YEAR **FIRST** SEMESTER EXAMINATION FOR DOCTOR OF PHILOSOPHY IN INFORMATION TECHNOLOGY

SIT 701– INFORMATION SECURITY AND GOVERNANCE

DURATION: 3 HOURS

DATE: 9/5/2019

TIME: 9-12 P.M.

Instructions to candidates:

1. Answer **Any Four** questions.
2. Mobile phones are not allowed in the examination room.
3. You are not allowed to write on this examination question paper.

QUESTION ONE (25 MARKS)

a) Explain FIVE reasons why it is difficult to protect information resources. (10marks)

b) Explain why the top- down approach to information security is superior to bottom – up approach. (5marks)

c) In the context of information security what are some of advantages for an organization adhering to requirements of specific standards. Also explain some possible shortcomings of standards in the context of information security. (10marks)

QUESTION TWO (25 MARKS)

a) Information security is a major concern for the software industry today as the number of security threats is nearly 80%. Explain the various security threats. (15marks)

b) Discuss the legal and ethical issues associated with information security. (10marks)

QUESTION THREE (25 MARKS)

a) Explain contingency planning and describe how it is different from routine management planning. Also enlist the components of contingency planning. (15marks)

b) List and describe the various risk mitigation options. (10marks)

QUESTION FOUR (25 MARKS)

a) Confidentiality, integrity and availability are core attributes in security. Explain these concepts. (6marks)

b) Company A and B of similar size are potential victims of cyber-attacks. Company A have implemented information security management system (ISMS) whereas company B have no ISMS in place and only use ad hoc information security management.

   i) What is an ISMS? (3marks)

   ii) Assuming both companies became victims of cyber-attacks and the damages were equal, explain the possible differences if any, in consequences and sanctions against management of the two companies. (6marks)

   iii) Explain any FIVE challenges faced in ISMS implementation. (10marks)

QUESTION FIVE (25 MARKS)

a) Define information security governance and explain the importance of information security governance framework to an organization. (15marks

b) Discuss how an organization institutionalizes its policies and practices using education, training and awareness programs. (10marks)