JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN INFORMATION TECHNOLOGY SECURITY AND AUDIT

1ST YEAR 1ST SEMESTER 2018/2019 ACADEMIC YEAR

KISUMU CAMPUS

COURSE CODE: **IIT 6114**

COURSE TITLE: **ASSURANCE CONTROLS AND COMPLIANCE MANAGEMENT**

EXAM VENUE: **STREAM: PHD IN IT SECURITY AND AUDIT**

DATE: **EXAM SESSION: SEPTEMBER – DECEMBER, 2018 SEMESTER**

TIME: 3.00 HOURS

INSTRUCTIONS:

1. **Answer 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 1: {20 MARKS}

a) Compliance monitoring is very instrumental aspect of Compliance Management. Highlight some of the key uses of compliance monitoring within an organization that heavily depends on information technology? (5 Marks)

b) Employees at all levels of the organization are required to be aware of relevant compliance obligations and implement controls in their day to day business activities, including to actively monitor and report compliance issues and incidents, which forms compliance culture. Discuss the initiatives used to support compliance culture in an organization. (5 Marks)

c) According to ***ISO 19600***, an effective Group compliance management system enables an entity to demonstrate their commitment to compliance and to comply with their compliance obligations. Identify and exhaustively discuss the approaches used to establish, implement, maintain, evaluate, and improve their compliance management system. (10 Marks)

QUESTION 2: {20 MARKS}

a) The functions to be performed in connection with the provision of the service or the use of data processing/IT systems must be defined. A distinction must be made here between two levels. Identify and briefly describe these two levels? (6 Marks)

b) The object of the data access control requirements is to ensure that only authorized persons can access the data which they are authorized to access, and to prevent the data from being manipulated or read by unauthorized persons. To achieve this, certain basic requirements need to be in place. Discuss these basic requirements comprehensively. (14 Marks)

QUESTION 3: {20 MARKS}

a) Governments have to contend with constantly changing technology, multiple compliance requirements, increasing complexity of information security, and changing threats. However, they can navigate these challenges and accomplish critical information security goals. Identify critical points that government officials can take into consideration in ensuring success in accomplishing information security goals? (10 Marks)

b) Kenya being one of the countries that is looking forward to accomplish critical information security goals. Discuss the milestones that Kenyan Government has achieved towards this? (10 Marks)

QUESTION 4: {20 MARKS}

a) Successful information security programs must be developed and tailored to the specific organizational mission, goals, and objectives. However, all effective security programs share a set of key elements. Identify and discuss ***at least five*** of these elements. (20 Marks)

QUESTION 5: {20 MARKS}

a) To design, develop, and implement an efficient and effective Data Governance for Privacy, Confidentiality and Compliance (DGPC) practices, organizations must define a set of guiding principles that can be applied in each core process. These principles include, but are not limited to, the data privacy and confidentiality principles. Discuss these guiding principles. (10 Marks)

b) People is one of the ***three*** components of Data Governance for Privacy, Confidentiality and Compliance (DGPC) initiative. With the aid of a chart/diagram, discuss people component entirely in the context of DGPC initiative. (10 Marks)