(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
2020/2021 ACADEMIC YEAR

SPECIAL/SUPPLEMENTARY EXAMINATIONS
YEAR THREE SEMESTER TWO EXAMINATIONS

FOR THE DEGREE OF
BACHELORS OF SCIENCE
(INFORMATION TECHNOLOGY)

COURSE CODE : BIT 325

COURSE TITLE : INFORMATION ASSURANCE AND SECURITY II

DATE: 07/01/2021 **TIME: 2.00 P.M. – 4.00 P.M.**

INSTRUCTIONS TO CANDIDATES

ANSWER **QUESTIONS ONE** AND **ANY OTHER TWO**

QUESTION ONE [COMPULSORY] (30 MARKS)

a) Differentiate between the following terms:

i. Threats, attacks and vulnerabilities **(3 Marks)**

ii. Security mechanism and security service **(2 Marks)**

iii. Security policy and ICT policy **(2 Marks)**

b) List down the three major types of security mechanisms. **(3 Marks)**

c) Identify the three steps of an internal audit process **(3 Marks)**

d) Explain the following terms with regards to information assurance and security and highlight their importance:

i. Confidentiality. **(1 Mark)**

ii. Integrity **(1 Mark)**

iii. Availability **(1 Mark)**

e) Differentiate between passive and active threats **(2 marks)**

f) The diversity and ever expanding use of IT applications have created a variety of ethical issues. Identify the four general categories of ethical issues in Information Technology that can affect an organization. **(4 marks)**

g) Management defines three types of security policy. Identify them. **(3 marks)**

h) Policies are living documents that must be managed and nurtured, and are constantly changing and growing. Identify the five major components for a good policy that makes it to remain viable and useful to an organization. **(5 marks)**

QUESTION TWO (20 MARKS)

a) What is Cybersquatting? **(2 marks)**

b) An attack is the actual attempt to violate security. It is the manifestation of the threat on an asset. With examples, illustrate the four ways in which we can classify communication attacks that interrupts the normal flow of information. **(8 marks)**

c) Organizations typically include data classifications in their security policy, or in a separate data policy. This aids them to identify the value of the data to the organization which is critical in data protection and helps to ensure data confidentiality and integrity. The policy identifies classification labels used within the organization and how the data owners can determine the proper classification and the personnel who should protect data based on its classification. With examples, explain the major ways in which we can classify information in an organization. **(10 marks)**

QUESTION THREE (20 MARKS)

a) Privacy can be defined as the right to be left alone and to be free of unreasonable personal intrusions. Examine the major types of threats that can affect information privacy. **(6 marks)**

b) An organization can create privacy codes and policies that can front guidelines with respect to protecting the privacy of customers, clients, and employees. Examine the two types of models that can be used in protecting privacy. **(4 marks)**

c) With the increasing rise of threats to information assets, there has emerged various strategies for risk management. With examples, examine the various risk management strategies. **(10 marks)**

QUESTION FOUR (20 MARKS)

a) Without threat modelling, protecting yourself is like "shooting in the dark". Threat modeling is a structured approach to identifying, quantifying, and addressing threats. With examples, explain the threat modeling processes and procedures. **(12 marks)**

b) Data ownership refers to both the possession of and responsibility for information. Loshin (2202) defined data ownership as the control of information that includes not just the ability to access, create, modify, package, derive benefit from, sell or remove data, but also the right to assign these access privileges to others. With Examples, examine the different categories of users that are responsible for data determination and ownership. **(8 marks)**

QUESTION FIVE [20 MARKS]

a) The ten domains of cyber security are derived from different topics about information security. Each of the ten domains concentrates on different aspects of system security. While most of the domains relate to what you can do to your network, some domains do not. Write down short notes on each of the TEN domains of IT Security **(20 Marks)**