20 20

(Knowledge for Development)

KIBABII UNIVERSITY

(KIBU)

UNIVERSITY EXAMINATIONS
2020/2021 ACADEMIC YEAR

SPECIAL/SUPPLEMENTARY EXAMINATIONS
YEAR THREE SEMESTER ONE EXAMINATIONS

FOR THE DEGREE OF
BACHELORS OF SCIENCE
(INFORMATION TECHNOLOGY)

COURSE CODE : BIT 313

COURSE TITLE : INFORMATION ASSURANCE AND SECURITY ASSURANCE

DATE: 21/01/2022 **TIME: 11.00 A.M- 1.00 P.M**

INSTRUCTIONS TO CANDIDATES

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

QUESTION ONE [COMPULSORY](30 MARKS)

a) Differentiate between the following terms in relation to information security.

i. Threat and Attack **(2 Marks)**

ii. Subject and Object **(2 Marks)**

iii. Computer security and Information security **(2 Marks)**

iv. Policy and Law **(2 Marks)**

v. Risk management and Risk control **(2 Marks)**

b) Several professional organizations have established codes of conduct/ethics. List down three code of ethics for an IT security professional. **(3 Marks)**

c) List down the three major steps in risk management **(3 Marks)**

d) Explain the following terms with regards to IT security:

i. Confidentiality. **(2 Marks)**

ii. Integrity **(2 Marks)**

iii. Availability **(2 Marks)**

e) What is a residual risk? **(1 Mark)**

f) List down the seven components of an IT Security policy document **(7 Marks)**

QUESTION TWO (20 MARKS)

a) A threat assessment process identifies and quantifies the risks facing each asset. Explain the four major steps in Risk Identification process. **(8 Marks)**

b) For each threat and associated vulnerabilities that have residual risk, it is important to create a preliminary list of control ideas. Examine the three general categories of controls.

(6 Marks)

c) Examine the five strategies used in risk control **(5 Marks)**

d) Explain the vulnerabilities associated with software as an enterprise information system component. **(1 Marks)**

QUESTION THREE (20 MARKS)

a) System specific policy (SysSPs) frequently functions as standards and procedures used when configuring or maintaining systems. Systems-specific policies fall into two groups. Explain. **(4 Marks)**

b) Examine the three level of controls found in a security architecture. **(6 Marks)**

c) In Business Impact Analysis (BIA), there is need to Investigate and assess the impacts that various attacks can have on the organization. Explain the stages of a BIA.

(10 Marks)

QUESTION FOUR (20 MARKS)

a) Contingency planning (CP) made up of three components. Explain **(6 Marks)**

b) Differentiate between a security procedure and a security policy and highlight the importance of each. **(2 Marks)**

c) Access controls are methods by which systems determine whether and how to admit a user into a trusted area of the organization. Examine the three major types of access controls used for information management in organizations. **(6 Marks)**

d) Explain any **three** best practices that can be exercised by a user to prevent possible damage to computer systems within the organization. **(6 Marks)**

QUESTION FIVE (20 MARKS)

a) Describe the defense in-depth (layered) architecture as a strategy for security effective implementation of information security and argue for its effectiveness. **(7 Marks)**

b) Examine three factors to consider when choosing the right firewall to secure an organizations' network. **(3 Marks)**

c) With examples, Differentiate between Honeypots, Honeynets and padded cell systems

(3 Marks)

d) Scanning and Analysis Tools are typically used to collect information that attackers would need to launch successful attack. Examine the tools that are valuable to a network in an organization. **(7 Marks)**