# KABARAK UNIVERSITY

## UNIVERSITY EXAMINATIONS

## 2015 / 2016 ACADEMIC YEAR

## FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN I.T SECURITY AND AUDIT

## ISEA 911: ADVANCE ISSUES IN INFORMATION SECURITY

**DAY: FRIDAY** **DATE: 11/12/2015**

**TIME: 9:00AM – 12:00PM** **STREAM:**

**INSTRUCTIONS:**

**Answer Question ONE (Compulsory) and any other TWO Questions**

**Question One (20 marks)**

a) It's known that the Cyberspace can be good or bad, what is your take? **(5 marks)**

b) Define defense in depth and list the components required to fulfill this endeavor? **(5 marks)**

c) Why is information security policy management important? **(2 marks)**

d) Differentiate between security policy, standards and guidelines? **(4 marks)**

e) Explain how public key cryptography may be used for identification. **(4 marks)**

**Question Two (20 marks)**

a) What do you understand by the term defense-in-depth? Using a diagram explain the various parts that form the defense in depth architecture. (**6 Marks**

b) Why do enterprise need Incident Response Planning to be put in place? (**3 Marks**

c) Why is Disaster Recovery Planning important in an enterprise? (**3 Marks**

d) Why is Business Continuity Planning important in an enterprise? **(3 Marks**

e) How do business protect themselves against natural disasters? **(5 Marks**

**Question Three (20 marks)**

a) In a high security setup it's advisable to deploy multifactor authentication (MFA), explain? **(4 marks)**

b) Identity management has become a separate consideration for access control with three factor required for successful access to the system: authentication, authorization, and accountability. Please explain? **(6 marks)**

c) In an organization in provisioning employs role-based job, why is important to put in place role based access control (RBAC)? **(3 marks)**

d) Differentiate between role-based access control (RBAC) and mandatory access control (MAC).

**(5 marks)**

e) In information security setup, it's known that "People" are the weakest link in an attempt to secure the network infrastructure. Explain. **(2 marks)**

**Question Four (20 marks)**

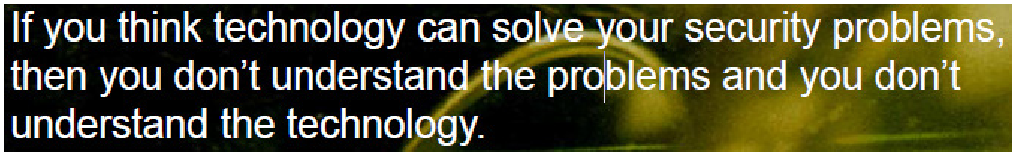
a) What are the common security frameworks? **(7 marks)**

b) What are the basic security concepts & principles in relation to information security & information assurance? **(7 marks)**

c) What are the key approaches to applying security concepts & principles? **(6 marks)**

**Question Five (20 marks)**

a) What is your take on the statement given below: **(4 marks)**



If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

b) Differentiate between information security versus compliance in information security? **(10 marks)**

c) What are the key factors in managing and mitigating security issues in an enterprise? **(6 marks)**

**Question Nine (Information Assurance)**

a) Under the design of security architecture, what is defense in depth? **(4 marks)**

b) Using a diagram explain the various parts that form the defense in depth architecture. **(6 marks)**

c) Schematically diagram show how you would secure your enterprise network, right from the Unknown network (the Internet) to LAN (the private network). Indicate where the internet facing servers are located and secure servers are placed. **(10 marks)**