UNITED STATES INTERNATIONAL UNIVERSITY

SCHOOL OF SCIENCE AND TECHNOLOGY

SPRING 2016 - MID SEMESTER EXAMINATION

COURSE: MIS 6130: INFORMATION SYSTEMS SECURITY, CONTROL AND AUDIT

INSTRUCTOR: BENSON MUTHOGA KIONI

TIME ALLOWED: 1 HOUR 40 MINUTES

MAXIMUM MARKS: 50

INSTRUCTIONS:

Read the following instructions carefully:

1. This exam is arranged in 2 Sections. Section A is COMPULSORY so answer ALL questions. Choose any TWO questions from Section B.
2. Start each question's answers on a NEW PAGE (you will be penalized if not done)
3. Marks for each question are indicated in brackets at the end of the question. They will be awarded to clear and logical answers
4. No plagiarism, copying or cheating will be tolerated. If done it will attract a 0 mark for this examination and further disciplinary action may be taken. Do NOT refer to unauthorized material in the examination room and do not access your mobile phones.
5. Write you **Student ID Number** and Name clearly on the answer sheet.
6. Write the number of Questions (and their Sub-Sections) on the answer booklet in the order you answered them. DO NOT MIX Sub-Sections of Questions. Completely answer a Question set before moving to the next Question.

Section A - Compulsory

Answer ALL in this Section

Question 1 (Compulsory) 30 Marks

a) Briefly describe the following Information Security Terms.
   i. File Hashing **(1 mark)**
   ii. Risk **(1 mark)**
   iii. DMZ **(1 mark)**
   iv. Threat **(1 mark)**
   v. Vulnerability: ` **(1 mark)**

b) What is a Security Kernel? **(2 marks)**

c) List and briefly describe the Seven Domains of a Typical IT Infrastructure **(7 marks)**

d) Define what a VoIP Gateway is and by using an illustration explain how the VoIP Gateway has contributed to savings for companies. **(6 marks)**

g) List and explain the Four Models of Access Controls **(10 marks)**

Aligned to CLO 1, 3 & 5 (Blooms Taxonomy Level [1] Knowledge, [2] Comprehension [3] Analysis)

Section B

Answer any TWO Questions from this Section

Question 2 (Optional)

a) Distinct between a BCP and a DRP **(5 marks)**

b) What are the requirements for an Information Security Policy to become enforceable? **(5 Marks)**

Aligned to CLO 1, 3 & 5 (Blooms Taxonomy Level [1] Knowledge, [2] Comprehension)

Question 3 (Optional)

a) What are the differences between a policy, a standard, and a practice? **(5 Marks)**

b) What are the three types of security policies and where would each be used? **(5 Marks)**

Aligned to CLO 1, 3 & 5 (Blooms Taxonomy Level [1] Knowledge, [2] Comprehension)

Question 4 (Optional)

a) State and briefly describe the two main Biometric Categories **(5 marks)**

b) List and describe the five Risk Control Strategies **(5 marks)**

Aligned to CLO 1, 3 & 5 (Blooms Taxonomy Level [1] Knowledge, [2] Comprehension)

Answers to Questions
Section A - Compulsory
Answer ALL in this Section
Question 1 (Compulsory) 30 Marks

Section A - Compulsory

Answer ALL in this Section

Question 1 (Compulsory) 30 Marks

a) Briefly describe the following Information Security Terms.

RESPONSE

I. File Hashing **(1 mark)**

Response: In file hashing, a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a hash value.

II. Risk **(1 mark)**

Response: Risk is the likelihood that something bad will happen to an asset.DMZ **(1 mark)**

III. Threat

Response: A threat is any action that could damage an asset. **(1 mark)**

IV. Vulnerability:

Response: A vulnerability is a weakness that allows a threat to be realized or to have an effect. **(1 mark)**

b) What is a Security Kernel (2 marks)

RESPONSE:

- The security kernel is the central part of a computing environment. It enforces access control for computer systems.
- The security kernel provides a central point of access control and implements the reference monitor concept.
- A reference monitor is software that provides a central point of processing for all resource access requests.

c) List and briefly describe the Seven Domains of a Typical IT Infrastructure (7 marks)

Response:

- User Domain
- Workstation Domain
- LAN Domain
- LAN-to-WAN Doman
- WAN Domain
- Remote Access Domain
- System/Application Domain

c) **Define what a VoIP Gateway is and by using an illustration explain how the VoIP Gateway has contributed to savings for companies. (6 marks)**

RESPONSE: VoIP Gateways are what connect different types of communication. In the past they were used to turn VoIP communication into normal analog communication. They had normal RJ-11 connectors in these Gateways. Savings: A gateway located in a remote office means the HQ will route their telephone calls through the normal internet/T1 connections that they have and at the remote office the VoIP Gateway will enable the call to be used as a local call thereby saving the company money.

g) **List and explain the Four Models of Access Controls** **(10 marks)**

Section B

Answer any TWO Questions from this Section

Question 2 (Optional)

a) Distinct between a BCP and a DRP. **(5 Marks)**

A Business Continuity Plan (BCP) is a plan for a structured response to any events that result in an interruption to critical business activities or functions. *The BCP addresses the processes, resources, equipment and devices needed to continue conducting critical business activities when an interruption occurs that affects the businesses's viability*.

A Disaster Recovery Plan (DRP) is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. *It is a comprehensive statement of consistent actions to be taken before, during and after a disaster*.

d) **What are the requirements for an Information Security Policy to become enforceable? (5 Marks)**

RESPONSE: For a policy to become enforceable, it must be:

1) Dissemination (distribution) - The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee.
2) Review (reading) - The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees.
3) Comprehension (understanding) - The organization must be able to demonstrate that the employee understood the requirements and content of the policy.
4) Compliance (agreement) - The organization must be able to demonstrate that the employee agrees to comply with the policy, through act or affirmation.
5) Uniform enforcement - The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Question 3 (Optional)

a) **What are the differences between a policy, a standard, and a practice? (5 Marks)**

RESPONSE: A policy is a plan or course of action intended to influence and determine decisions, actions, and other matters. Policies are organizational laws because they dictate acceptable and unacceptable behavior within the context of the organization's culture. A standard, like a policy, has the same requirement for compliance, but it provides more detail as to what must be done to comply with policy. The level of acceptance of standards may be informal (as in de facto standards) or formal (as in de jure standards). Finally, practices, procedures, and guidelines effectively explain how to comply with policy. *Policies provide instructions on what technologies can and cannot be used for. Three criteria for shaping sound policies are:*

- Never conflict with law
- Stand up in court, if challenged
- Be properly administered through dissemination and documented acceptance

For these reasons, it is important for policy to be adequately detailed to ensure proper implementation.

Policy that is not well defined can cause significant liability for the company if it finds itself defending policy in a court of law. Unless a particular use is clearly prohibited, the organization cannot penalize an employee for its misuse.

Policy has the ultimate responsibility for managing technology. System administrators and users are responsible for enforcing policy.

b) What are the three types of security policies and where would each be used? (5 Marks)

Based on The National Institute of Standards and Technology's (NIST) Special Publication 800-14, there are three types of information security policies.

First are **general or security program policies (SPP),** which are usually drafted by the chief information officer of the organization. The SPP are used to directly support the mission, vision, and direction of the organization and set the strategic direction, scope, and tone for all security efforts within the organization.

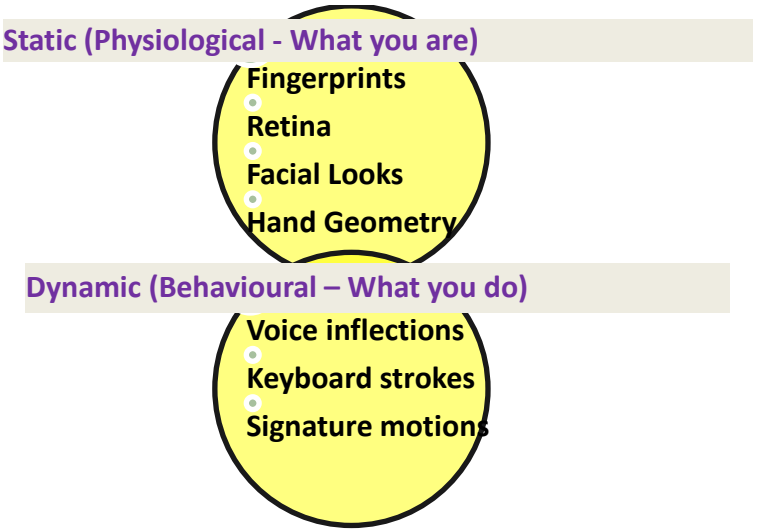
Second are **issue-specific security policies (ISSP)** that are formally written to instruct employees to properly use the technologies of the organization such as use of the Internet, electronic email, and use of photocopy equipment. The ISSP requires frequent updates and must contain a statement on the organization's position on a specific issue.

Third are **system-specific security policies (SysSP).** The SysSP are not formal documents but are usually codified as standards and procedures used when configuring or maintaining

systems. The SysSP fall into two groups: access control lists and configuration rules.

Question 4 (Optional)

a) **State and briefly describe the two main Biometric Categories** **(5 marks)**



b) **List and describe the five Risk Control Strategies** **(5 marks)**

RESPONSE:

1. *Defend* - The defend control strategy attempts to prevent the exploitation of the vulnerability.
2. *Transfer* - The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations.
3. *Mitigate* - The mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.
4. *Accept* - The accept control strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation.
5. *Terminate* - The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks.