UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE: **IT08X47/IT8X298**
INFORMATION SECURITY
CAMPUS: **APK**
ASSESSMENT: **FINAL SUMMATIVE ASSESSMENT. JUNE 2020**

DATE	2 JUNE 2020	**SESSION**	Morning
INTERNAL EXAMINER		Dr. J du Toit	
EXTERNAL EXAMINER		Prof L Futcher	
DURATION 2 Hours		**MARKS** 100	

Please read the following instructions carefully:

1. Write clearly and legibly.
2. Answer all questions.
3. This paper consists of 4 pages
4. This is an open book assessment. You may consult your notes and textbook during the assessment.
5. You are **NOT** allowed to copy from any notes.
6. You are **NOT** allowed to assist or gain assistance from anyone else.

QUESTION 1 (The need for security) [18]

You have recently been employed as the Information Security (IS) Engineer at the Utopian Centre for Communicable Diseases (UCCD). After a recent audit, the UCCD are concerned about their IS exposure. You have decided to focus on the most prevalent threats to the UCCD IS systems and address those threats first. (18)

Write a plan that addresses the three most prominent IS threats that you could identify.

For each threat:

- Describe in which threat category it falls.
- Why that threat is specifically a problem for UCCD
- What controls you will implement to address the specific threat.

Marks are awarded as follow:

- Listing of three threats. One mark per threat (3).
- Threat categorisation. One category per threat (3).
- Justification of threat. Two marks per threat (6).
- Control of threat. Two marks per control (6).

QUESTION 2 (Information Security Planning) [15]

The audit mentioned that the IS policies, *for who the board of directors are responsible*, were last updated five years ago. The company is preparing to outsource the creation of the IS policies to an external service provider. You have been asked to help prepare a request for quote (RFQ). You have been tasked to prepare the section of the RFQ that focusses on the different types of policies. (15)

Write a section of the RFQ that highlights the different types of policies. For each of the different types of policies argue whether the type of policy should be included in the scope for the work covered by the service provider.

Marks are awarded as follow:

- Listing of the three types of IS policies. One mark per policy type. (3)
- Description of each policy type. Two marks per policy type. (6)
- Argument of whether the policy type should be included in the scope. Two marks per policy type (6)

QUESTION 3 (The five information security services) [15]

The CEO of UCCD recently read an article on zero-trust network architectures. The CEO knows that ISO 7498/2 is the five information security services that underpins most of the UCCD's system designs. (15)

Write a MEMO where you explain how the principle of zero-trust can be applied to each of the five IS services . If you feel that the principle of zero-trust does not apply to a specific IS service, then you must provide an explanation of why that may not be the case.

Marks are awarded as follow:

- Listing and providing a basic description of the 5 IS services (5)
- Relate how zero-trust is applicable in each of the 5 IS services (10)

QUESTION 4 (Digital Signatures, Confidentiality and Non-Repudiation) [42]

The UCCD would like to implement and design a system that will allow hospitals and private health care practitioners to send and receive information about communicable diseases to the UCCD. It is your responsibility as the IS Engineer for UCCD to define the security requirements and define a process that will describe how the system will implement the requirements. The focus of the requirements should be on integrity, confidentiality and non-repudiation. (42)

Write a design document that consists of three major sections:

- **Section 1**: Highlight and specify the various security requirements that the system should adhere to.
- **Section 2**: A detailed process that describes how the security is established in the system, given the security requirements.
- **Section 3**: Critically evaluate the design and determine which section of the system may still be at risk.

Marks are awarded as follow:

Section 1:

- Describing at least three security requirements. (6)

Section 2:

- Structured approach. (3)
- Clearly describing and highlighting different security keys (4)
- Process designed to fulfil the requirements (17)

Section 3:

- Discussing risks inherent in the existing design (7)
- At least three risks must be identified.

Overall neatness and readability (5)

QUESTION 5 (Confidentiality) **[10]**

5.1 Given the following clear text alphabet and polyalphabetic substitution cipher. **Write** the cipher text for the word: ***SING*** (2)

`Clear Text`	`ABCDEFGHIJKLMNOPQRSTUVWXYZ`
`Substitution cipher 1:`	`DEFGHIJKLMNOPQRSTUVWXYZABC`
`Substitution cipher 2:`	`GHIJKLMNOPQRSTUVWXYZABCDEF`
`Substitution cipher 3:`	`JKLMNOPQRSTUVWXYZABCDEFGHI`
`Substitution cipher 4:`	`MNOPQRSTUVWXYZABCDEFGHIJKL`

5.2 Write the cipher text when a permutation cipher is applied to the following clear text given the following permutation key. (2)

Permutation key: **1 -> 2; 2 -> 5; 3 -> 1; 4 -> 3; 5 -> 4**

Clear text: ***SMILE***

5.3 **Discuss** three problems with keys used in symmetric encryption (6)

TOTAL PAPER **[100]**