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	JUNE 2020	**SESSION**	Morning
INTERNAL EXAMINER		Mr. 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 6 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.

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).

Threats should be real-world threats. This can include many things such as Phishing attacks, Password re-use, man-in-the-middle attacks, denial-of-service attacks etc.

The categories that students can choose from is:

- Compromises to intellectual property
- Deviations in equality of service
- Espionage or trespass
- Forces of nature
- Human error or failure
- Information extortion
- Sabotage or vandalism
- Software attacks
- Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolescence
- Theft

The justification of threat must answer the question "Why" is the threat a problem.

The control of the threat can be a general control that can be implemented. It must specifically apply to the threat.

QUESTION 2 (Information Security Planning) **[15]**

The audit also 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)

Enterprise IS Policy

Executive level document. Sets the responsibilities and penalties and disciplinary actions.

Should be included in the RFQ. EIS Policy must be approved by the board.

Issue-specific security policy

Addresses specific areas of technology. Requires frequent updates. Contains statements on the organisation's position on a specific issue.

Must be included in the RFQ, since it defines the organisation's position and require the board to approve.

System-specific security policy

Acts as standard or procedures when configuring or maintaining a system. Provides managerial guidance or technical guidance.

My or may not be included in the RFQ, but most of these policies apply to a system specifically which is normally part of the IT department's responsibilities. Not normally part of the responsibility of the board.

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

The CEO 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 .

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)

The student should list the five information security services.
For each service the following aspects could be considered.

Identification and Authentication:

- Before any connection is established.
- There must be positive identification
- There may multiple factors of identification and authentication.
- There may also be multiple levels of identification and authentication in the network stack.

Authorisation:

- Levels of access may depend on the level of identification and authentication
- The more critical the data, the more verification is required (factors of identification and authentication)

Integrity:

- Zero trust uses the principle of never trust, always verify.
- The principle that data also needs to be verified before it can be trusted.
- The two nodes must have the capacity to detect when data has been tampered with.

Confidentiality:

- There must be some level of assurance that data can only be accessed between two parties.
- Connections occur over untrusted network zones, which means confidentiality must be applied on the higher levels to ensure

Non-repudiation:

- The principle of zero-trust continues even after transactions occurred.
- Transactions must be linked to specific nodes.
- Nodes should not have the ability to deny performing a transaction in the future.
- Even after verification occurred, any transaction must be linked to a specific node. This ensures that nodes cannot deny

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)

Section 1: Many requirements may be listed here. They may include:

- Withstand man-in-the-middle attacks.
- Ensure perfect forward secrecy.
- Integrity of messages must be assured.
- All messages must be confidential.
- System must ensure non-repudiation.
- Other requirements, such as positive identification and authentication and authorisation, may also be given.

Section 2: This is dependent on the requirements.

- Man-in-the-middle attack: HMAC that is signed by the sender to verify integrity and authentication.
- Ensure perfect forward secrecy: Solution must make use of Ephemeral keys, using Diffie-Hellman
- Integrity of message: Each message must have a MAC (Key with the message).
- Confidentiality: Student should try and use symmetric key encryption for confidentiality, but half marks may be given for asymmetric key encryption.
- Non-repudiation: Must make use of PKI and messages must be digitally signed.

Section 3: Three IS risks

- Evaluation, must identify and discuss three risks.

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

VOWS

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***

ISLEM

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

Size:

The smaller the key the less effort it is to brute force attack.

Distribution:

Both the sender and receiver needs the same key. The question is always how the key should be distributed between the two parties, that can guarantee the confidentiality of the key.

Derivation:

If a key is derived from a short or simple password, then an attacker can also derive the key, if they know the parameters.

TOTAL PAPER **[100]**